**Statement of Work (SOW)**

**N66001-22-F-3509**
**In-Service Engineering Activity (ISEA)**
**Naval Enterprise Networks (NEN) Contract**
**NIWC Pacific San Diego**
**05 August 2022**

## 1.0 INTRODUCTION:

The effort provides support for Code 41260, the Shore Networks Branch. The branch is responsible for the requirements, design, development, accreditation, integration, modernization, sustainment, upgrade and Life Cycle Support (LCS) of shore networks, network components and network service solutions for Navy and Joint Department of Defense (DoD) shore units worldwide.

## 1.1 SCOPE

This Statement of Work (SOW) for the In-Service Engineering Activity (ISEA) Navy Enterprise Networks (NEN) includes the four core Capability-Based (CB) In-Service Engineering Activity (CB-ISEA) services: Technical Sustainment Support (TSS), Sustainment Engineering Support, Logistics Support, and Modernization Support. The contract requirements are to provide the following services: (1) Integrated Project Team and Project Management, (2) Sustainment Engineering Support, (3) Technical Sustainment Support, (4) Integrated Logistics Support (ILS), (5) Configuration Management (CM), (6) Certification and Accreditation (C&A), (7) System Implementation and Upgrade, (8) Enterprise Applications (EAs) Support, (9) Work Baseline Software Configuration (WBSC) Support, and (10) Tier IV OCONUS Support.

Specific taskings will be generated and defined through issuance of technical direction letters.

The effort requires the integration, testing, implementation and use of a significant amount of Information Technology (IT) software [Operating System (OS), applications, software development and scripting] and hardware [Personal Computers (PCs), servers, network devices (switches, routers, firewalls, load balancers, proxy appliances, etc.), and other peripheral Commercial Off-the-Shelf (COTS), Government off the Shelf (GOTS) and Non Developmental Items (NDI)] for each of the programs supported; as listed below. The effort also includes the procurement of incidental materials. Any replacement, follow-on, or interrelated system associated with the systems listed below will be covered by the scope of this SOW.

- GIG - Global Information Grid
- ONE-Net - OCONUS Navy Enterprise NETwork
- NGEN - Next Generation Enterprise Network
- NEN - Navy Enterprise Network

## 2.0 APPLICABLE DOCUMENTS

The following documents are referenced for guidance only and form a part of the statement of work to the extent specified herein. Unless otherwise specified, the issues of the documents below will be those listed in the Department of Defense Index of Specifications and Standards (DoDISS) and supplement thereto, cited in the solicitation. The document to be used shall be the issue in effect at the award of each task order. In the event of a conflict between this statement of work and the documents herein, the text of the statement of work will take precedence. Nothing in this statement of work however, shall supersede applicable laws and regulations, unless a specific exemption has been obtained.

### 2.1 OPTIONAL MILITARY SPECIFICATIONS:

| | |
|---|---|
| MIL-DTL-17J | Cables, Radio Frequency, Flexible and Semi rigid, General Specification For |
| MIL-DTL-15024F | Plates, Tags, and Bands for Identification of Equipment, General Specification for |
| MIL-DTL-24784C | Manuals, Technical: General Acquisition and Development Requirements, General Specification for |
| MIL-E-17555H | Electronic and Electrical Equipment, Accessories, and Provisioned Items (Repair Parts): Packaging Of |
| MIL-PRF-85337B | Manuals, Technical: Quality Assurance Program; Requirements for |
| MIL-PRF-16552F | Filter, Air Environmental Control System, Cleanable, Impingement (High Velocity Type) |
| MIL-PRF-29612B | Training Data Products |
| MIL-PRF-32216A | Evaluation of Commercial Off The Shelf (COTS) Manuals and Preparation of Supplemental Data |

### 2.2 OPTIONAL MILITARY STANDARDS:

| | |
|---|---|
| MIL-STD-129R | Military Marking for Shipment and Storage |
| MIL-STD-130N | Identification Marking of U.S. Military Property |
| MIL-STD-202G | Test Method Standard Electronic and Electrical Component Parts |
| MIL-STD-461F | Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment |
| MIL-STD-810G | Environmental Engineering Considerations and Laboratory Tests |

| | |
|---|---|
| MIL-STD-882E | System Safety |
| MIL-STD-883J | Test Method Standard, Microcircuits |
| MIL-STD-961E | Defense and Program-Unique Specifications Format and Content |
| MIL-STD-1472G | Human Engineering |
| MIL-STD-1474D | Department of Defense Design Criteria Standard- Noise Limits |
| MIL-STD-1686C | Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices) |
| MIL-STD-1840C | Automated Interchange of Technical Information |
| MIL-STD-2073-1E | (1) Standard Practice for Military Packaging |
| MIL-STD-2110 | Restoration, Overhaul, and Repair of Electronic Equipment |
| MIL-STD-3034A | Reliability-Centered Maintenance (RCM) Process |
| MIL-STD-31000A | Technical Data Packages |
| MIL-STD-38784A | Manuals, Technical: General Style and Format Requirements |
| MIL-STD-46855A | Human Engineering Requirements for Military Systems, Equipment and Facilities |

2.3 **OPTIONAL MILITARY HANDBOOKS:**

| | |
|---|---|
| MIL-HDBK-61A | Configuration Management Guidance |
| MIL-HDBK-217F | Reliability Prediction of Electronic Equipment |
| MIL-HDBK-237D | Electromagnetic Environmental Effects and Spectrum Supportability Guidance for the Acquisition Process |
| MIL-HDBK-347 | Mission Critical Computer Resources Software Support |
| MIL-HDBK-419A | Grounding, Bonding and Shielding for Electronic Equipments and Facilities |
| MIL-HDBK-454B | General Guidelines for Electronic Equipment |
| MIL-HDBK-470A | Designing and Developing Maintainable Products and Systems MIL-HDBK-502A Product Support Analysis |
| MIL-HDBK-781A | Reliability Test Methods, Plans, and Environments for Engineering Development, Qualification, and Production |
| MIL-HDBK-831A | Preparation of Test Reports |
| MIL-HDBK-2036 | Electronic Equipment Specifications, Preparation of |

| | |
|---|---|
| MIL-HDBK-2097A | Acquisition of Support Equipment and Associated Integrated Logistics Support |
| MIL-HDBK-2155 | Failure Reporting, Analysis and Corrective Action Taken |
| | MIL-HDBK-2165 Testability Program for Systems and Equipments |
| MIL-HDBK-29612/4A | Glossary for Training |

2.4 **OTHER DOCUMENTS:**

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI)

| | |
|---|---|
| ANSI/ISO/ASQ Q9001-2008 | Quality Management Systems Requirements Standard |
| ANSI/ASQC Q9004-1 | Quality Management and Quality System Elements |
| | TechAmerica/ANSI EIA-649B National Consensus Standard for Configuration Management |
| ANSI X3.131-1986 | Small Computer System Interface (SCSI) |
| SCSI-2 Rev 10L | Small Computer System Interface - 2 (SCSI-2) |

AMERICAN SOCIETY OF MECHANICAL ENGINEERS (ASME)

| | |
|---|---|
| ASME Y14.100 | Engineering Drawing and Related Documentation Practices |
| ASME Y14.44 | Reference Designations for Electrical and Electronic Parts and Equipment |

AMERICAN SOCIETY FOR TESTING AND MATERIALS (ASTM)

| | |
|---|---|
| ASTM D3951-10 | Standard Practice for Commercial Packaging |

ELECTRONIC COMPONENTS INDUSTRY ASSOCIATION (ECIA)

| | |
|---|---|
| EIA/ECA-310-E | Cabinets, Racks, Panels, and Associated Equipment |

INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS (IEEE)

| | |
|---|---|
| IEEE 100 | The Authoritative Dictionary of IEEE Standards Terms Seventh Edition |
| IEEE 260.1 | Letter Symbols for Units of Measurement (SI Units, Customary Inch-Pound Units, and Certain Other Units) |

| | |
|---|---|
| IEEE 280-1985 | IEEE Standard Letter Symbols for Quantities Used in Electrical Science and Electrical Engineering, |
| IEEE 315-1975 | Graphic Symbols for Electrical and Electronics Diagrams (Including Reference Designation Class Designation Letters) (ANSI Y32.2) |
| IEEE 315A-1986 | Supplement to Graphic Symbols for Electrical and Electronic Diagrams INTERNATIONAL STANDARDS ORGANIZATION (ISO) |
| ISO 9001:2008 | Quality Management Systems SAE INTERNATIONAL |
| SAE-GEIA-STD-0007 | Logistics Products Data |

2.5 **OTHER DoD and NAVY DOCUMENTS:**

COMUSFLTFORCOMINST Joint Fleet Maintenance Manual (JFFM) 4790.3 REV C

| | |
|---|---|
| DOD 4104.1-R, 23 May 2003DOD | Supply Chain Materiel Management Regulation |
| DoD 5220.22-M, 28 Feb 06 | National Industrial Security Program Operating Manual |
| DoDD 8140.01, 11 Aug 15 | Cyberspace Workforce Management |
| DoDI 8320.04, 16 Jun 08 | Item Unique Identification (IUID) Standards for Tangible Personal Property |
| DoDI 8500.01, 14 Mar 14 | Cybersecurity |
| DoDI 8500.2 6 Feb 03 | Information Assurance (IA) Implementation |
| DoDI 8510.01, 12 Mar 14 | Risk Management Framework (RMF) for DoD Information Technology (IT) |
| DoDD 8570.01 15 Aug 04 | Information Assurance Training, Certification, and Workforce Management |
| DoD 8570.01-M Change 3 | Information Assurance Workforce Improvement Program 24 Jan 12 |
| FTR – P/O 41 | Code of Federal Regulations (CFR) Chapters 300-304 Federal Travel Regulation |

| | |
|---|---|
| JTR Vol II | Joint Travel Regulations, Volume 2, DOD Civilian Personnel |
| N65236-LOG-EPROC-0095-1.0 | Tier IV Escalation Process - SSC LANT Fleet & Customer Support Process 12 Sep 11 |
| NAVADMIN 107/12, 29 Mar 12 | Navy Information Assurance Workforce and Operating System/Computing Environment Certifications |
| NAVICPINST 4441.170B CH-1 | COSAL Use & Maintenance Manual Mar 2009 |
| NAVSEA SL720-AA-MAN-010 | Fleet Modernization Program (FMP) Management and Operations Manual |
| NSTS 9090-700 | NAVSEA Technical Specification Configuration Data Manager's Database-Open Architecture (CDMD-OA) |
| NAVSUP P-485 VOLUME III | Naval Supply Procedures - Ashore Supply |
| NAVSUP P-545 | Depot Level Repairable Requisitioning, Turn-In and Carcass Tracking Guide |
| OPNAV 4790.4E | Ship's Maintenance and Material Management (3-M) System Policy |
| SD-2, 1 Jan 10 | Buying Commercial & Nondevelopmental Items - A Handbook |
| SD-5, Jan 2008 | Market Research Gathering Information About Commercial Products and Services |
| SECNAVINST 5100.10J | Department of the Navy Policy for Safety, Mishap Prevention, 26 Oct 2005 Occupational Health and Fire Prevention Programs |
| SECNAVINST 5239.19, Mar 08 | Incident Response |
| SECNAVINST 5239.20A, 10 Feb 16 | DON Cyberspace IT and Cybersecurity |
| SECNAVINST 5239.3C, 2 May 16 | DON Cybersecurity Policy |
| SECNAV M-5239.2, May 2009 | DON Information Assurance Workforce Management Manual |

| | |
|---|---|
| UTNP Policy, V1.0, 31 Oct 02 | OPNAV Navy-Marine Corps Unclassified Trusted Network Protection (UTN- w/Changes Protect) Policy |
| NAVNETWARCOM / SPAWARSYSCOM New C&A Process Guide Version 1.0 of 8 Jul 08 | |
| NAVSEA Program Support Data (PSD) Automated Reporting and Tracking System (PARTS) User's Manual, 1 Mar 04 | |
| Navy Ports, Protocols, and Services (NPPS) Manual | |
| SPAWAR Shore Installation Process Handbook (SIPH) | |
| SECNAVINST 5510.30C | Department of Navy Personnel Security Program, 24 January 2020 |
| SECNAVINST 5510.36B | DON Information Security Program, 12 July 2019 |
| OPNAVINST F3300.53C | Navy Antiterrorism Program, May 2009 |
| DODM 5200.01, Volume 1 | DoD Information Security Program: Overview, Classification, And Declassification, Ch-2 28 July 2020 |
| DODM 5200.01, Volume 2 | DoD Information Security Program: Marking Of Classified Information, Ch-4 28 July 2020 |
| DODM 5200.01, Volume 3 | DoD Information Security Program: Protection Of Classified Information, Ch-3 28 July 2020 |
| DODI 5200.48 | Controlled Unclassified Information (CUI), dated 6 March 2020 |
| DOD 5220.22-M (Series) | National Industrial Security Program Operating Manual (NISPOM), February Ch-2 18 May 2016 |
| DoDM 5200.02 | Procedures for the DoD Personnel Security Program (PSP) dtd 3 Apr 17 |
| NSDD 298 | National Security Decision Directive, National Operations Security Program, 22 January 1988 |
| DOD 5205.02-M | DOD Operations Security (OPSEC) Program, 3 November 1988, Ch-1, 26 April 2018 |

| | |
|---|---|
| DON CIO Memorandum, 12 Feb 16 | Acceptable Use of Department of the Navy Information Technology (IT) |
| NTD 10-11 | Navy Telecommunications Directive, System Authorization Access Request (SAAR) - Navy |
| OPNAVINST 3432.1DON | Operations Security, 4 November 2011 |
| SPAWARINST 3432.1 (Series) | Operations Security Policy, 2 February 2005 |
| SPAWARINST 4720.1A | SPAWAR Modernization and Installation Policy |
| NIWCPACINST 5500.1C Ch-1 | Security Manual, 25 September 2019 |

**3.0 TECHNCIAL REQUIREMENTS:**

*Begin OPN Sections*

3.1 **INTEGRATED PROJECT TEAM and PROJECT MANAGEMENT SUPPORT:** For the production engineering, installation of new capabilities and procurement of IT systems, the contractor shall:

3.1.1 Task Status Reports: For each task the contractor shall provide monthly progress and status reports. This report shall include reconcilable expenditure reports that shall track back to the initial quotation. **(CDRL A001)**

3.1.2 Management Reviews: The contractor shall provide project management support for the task orders issued under this contract and participate in and support program reviews held by NIWC Systems Pacific (NIWC PAC). This support shall include generating meeting minutes, identifying and tracking outstanding actions, management documentation, such as a Project Management Plan, Project-Level Integrated Master Schedule (IMS), Work Breakdown Structure (WBS) and individual Plan of Action and Milestones (POA&M), development/updates and all other matters to ensure the successful execution of all work to be performed on the task orders. **(CDRL A008/A009)**

3.1.3 Work with IPT lead and members to identify and prioritize tasks for the team; review progress; participate in meetings; review, track and process action items; and provide production engineering assessments and technical verification and validation of the capabilities and deficiencies of the systems and vendors.

3.1.4 Assess current and future system and software project requirements, analyze changes and situations and develop, and propose or recommend tentative approaches and solutions using a variety of tools, techniques, or processes.

3.1.5 Provide input for the preparation and presentation of briefing material and development of various program, system and business development documents.

3.1.6 Assess progress and identify schedule and technical variances and provide milestone support for major project efforts and facilitate and document project team activities. Documentation produced or modified shall be in the appropriate format and maintained in the electronic folders resident on the local area network. **(CDRL A001)**

3.1.7 Provide meeting minutes and an action item tracker for all meetings led by the contractor or in which the contractor attends in a supporting role. The contractor shall

consolidate all action item data in a central location on a NEN collaboration tool. **(CDRL A009)**

3.1.8 Conduct technical, cost, and schedule risk assessments.

3.2 **SUSTAINMENT ENGINEERING SUPPORT:** For the production engineering, installation of new capabilities and procurement of IT systems, the contractor shall:

3.2.1 Technical Support: The contractor shall conduct and/or participate in technical reviews. The contractor shall coordinate meetings, developing agenda items, participate in meetings, generate minutes, and track action items as required. The contractor shall develop and/or revise the following documentation; Request for Change (RFC), Specification Change Notices (SCN), Engineering Change Request (ECR), Engineering Change Notice (ECN), Fleet Readiness Certification Board (FRCB), and Field Changes (FCs). The contractor shall coordinate, attend and participate in site surveys, installations, implementations, technical assistance, meetings and conferences, and exchange information with program managers, engineers and users. The contractor shall support customers worldwide in different time zones and attend meeting at different times to support program requirements. **(CDRL A001/A009)**

3.2.2 System Evaluations and Trade Study Support: The contractor shall perform system evaluations/analysis, requirement reviews, Technology Readiness Level (TRL) Analysis, product evaluations, risk analysis, security evaluations and analysis to include Certification Test and Evaluations (CT&E) and Site Test and Evaluation (ST&E), decision papers, business case analysis or trade studies to determine where changes might be recommended to correct deficiencies, new product recommendation, achieve cost savings or improve operations and maintenance.

3.2.3 Design Analysis Support: The contractor shall provide plans, design analysis and recommendations for the following: Information Systems, Certification and Accreditation (C&A) Safety; Human Factors; Reliability, Maintainability, Availability, Heating/Cooling; Control of electrostatic discharge and Mercury contamination; and Power or Power Distribution.

3.2.4 Mockup Support: The contractor shall develop, document, validate, and maintain engineering mockups for specific system/equipment in accordance with specific system/equipment specification(s).

3.2.5 Engineering Development Model (EDM) Support: The contractor shall develop, document, validate, test and deliver EDMs for IT systems or equipment in accordance with specific system/equipment specification(s). EDM development shall identify operational and security configuration, integration, deployment and life cycle support equipment requirements.

3.2.6 Engineering Information Bulletins/Article(s) Support: The contractor shall develop and prepare periodic articles for inclusion into Newsletter(s), Standard Operating Procedures (SOPs) and Engineering Information Bulletins.

3.2.7 Drawing Support: The contractor shall develop drawing packages using existing packages to the maximum extent. The contractor shall develop, validate, modify, maintain, and utilize drawing packages, drawing trees (interrelationship of engineering drawings and associated lists), “As-Built” drawings, red-lined drawings,

Installation Control Drawings (ICD), Installation Design Plans (IDP) and block diagrams (schematic and functional, including all interfaces) using computer aided design software compatible with existing formats.

3.2.8 Mission Critical Computer Resources (MCCR) Support: The contractor shall develop, procure, document, test, and maintain any required MCCR and computer resources support.

3.2.9 Systems Support: The contractor shall provide support in developing, maintaining, documenting, integrating, and installing upgrades to shore systems that enables voice, video and data transmissions from any PC throughout the Navy. This will allow warfighters to exchange classified, unclassified, tactical or non-tactical information. The contractor shall develop, modify, operate, test, implement, document, and maintain Automated Information Systems (AIS). The contractor shall provide AIS services on a variety of systems and specialized workstations (i.e. computer-aided design) to include the following: (1) entry of data; (2) extracting, interpreting, editing and consolidating data; (3) designing, setting-up and implementing special input formats; (4) transmitting and receiving data; (5) documenting procedures for inputting data; (6) controlling the receipt and transmission of data; (7) specification of outputs; (8) operation of information system equipment; (9) design, implementation and management of databases; and (10) security. The contractor shall provide networking services that support the transfer of data, video, imagery and multimedia. The contractor shall provide the capability to manage network objects such as host computers, routers, local area networks, and wide area networks.

3.2.10 Rapid Prototyping Support/New Developmental Item: The contractor shall provide rapid prototyping support between new designs and modernization. This shall include the engineering, integration, documentation, and fabrication of enough subassemblies and assemblies that constitute either parts of or an entire system/suite as required to support the design validation and documentation verification and validation processes prior to full modernization. **(CDRL A004)**

3.2.11 Network Response Group (NRG): The contractor shall provide a NRG as necessary to support a limited rapid response to specific fleet technical assistance requirements. This response shall include the capability to diagnose and repair the complete network, end-to-end. This shall include, at a minimum, the computer networks, fiber optics, microwave, baseband, and all interconnections of the system network.

3.2.12 Network Systems Engineering: The contractor shall provide systems engineering support in the form of the development of technical insertions and solutions to supported systems. This support shall include; development and review of 400 series documents (High Level Architecture, Detailed Design, Requirements and Configuration Settings, Installation Procedures, Test Plans, Test Reports), Engineering Change Order (ECO), Bill of Materials (BoM), Operations Guidelines, Operations Procedures, Request for Changes (RFCs) and other technical documentation as required. Develop and review design, technical reports, cost estimates, and correspondence including letters and messages. Prepare and review design proposals, security documents, verify Installation Design Plans (IDPs)/drawings, and ensure specifications and design meet performance requirements. **(CDRL A003/A004)**

3.2.13 Prepare report(s), which include success criteria for installations, lessons learned/best practices, and improvement of fielded subsystems in terms of operability, technical merit, and schedule risks. **(CDRL A007)**

3.2.14 Create, modify, and/or update specifications and interface documentation to describe the physical, functional, and performance interfaces; and hardware, software, and system-level performance requirements. Documentation of information systems shall include preparing or updating system engineering plans (SEP), technical manual, operation and maintenance manuals, style guides, test plans, test reports, implementation plans, recommendations, bulletins, outlines and white papers in accordance with NEN standards. **(CDRL A006)**

3.3 **TECHNICAL SUPPORT:** For the production engineering, installation of new capabilities and procurement of IT systems, the contractor shall:

3.3.1 Technical Assistance Site Support: The contractor shall provide site support to determine the root cause of technical issues affecting system performance. The contractor shall coordinate with Government site personnel during the execution of the requirement. The contractor shall provide recommendations, correct issues, verify correction, document changes in relevant and applicable system configuration documents, and provide a final trip report documenting analysis, findings, corrected action, site points-of- contact, required documentation changes, and changes to applicable network devises. The contractor shall provide on-call 24/7 support (via telephone, chat or e-mail) and on-site (travel) services on equipment/systems to perform troubleshooting, correct CASREPs, provide Tier IV assistance, checkout, repair, and test worldwide. **(CDRL A003)**

3.3.2 Quality Assurance and Testing:

3.3.2.1 Quality Assurance (QA) Program: The contractor shall provide and maintain a quality/inspection system that, as a minimum, adheres to the requirements of ISO 9001:2008 or equivalent and supplemental requirements imposed by this contract. ISO 9001:2008 registration and certification will be considered as one method of proof of compliance with this requirement.

The quality system shall be documented and contain procedures, planning, and all other documentation and data necessary to provide an efficient and effective quality system based on their internal auditing system. The quality system shall be made available to the Government for review during predetermined visits. Existing quality documents that meet the requirements of this contract may continue to be used. The Government reserves the right to witness any specified inspections, installations, demonstrations, tests, validations, and verifications. The Government reserves the right to disapprove the contractor's and/or subcontractor's quality system or portions thereof when the quality system(s) fails to meet contractual requirements at either the program or worksite services level. The documented quality assurance system shall be used to ensure that the end product of each task

conforms to contract requirements whether produced by the contractor or provided by approved subcontractors or vendors. The quality assurance system shall provide for control over all phases of the various types of tasks, from initial manning and material ordering to completion of final tasking, before offering to the Government for acceptance as specified in this contract or task orders/PWS. All services shall be rendered according to the documented quality system and directly supervised by individuals qualified in the relevant profession or trade. **(CDRL A004)**

3.3.2.2 Quality Control: Unless otherwise directed, the contractor is responsible for all quality control inspections necessary in the performance of the various tasks as assigned and identified by the respective Work Breakdown Structure (WBS), POA&M or procedural quality system document. The Government reserves the right to perform any inspections deemed necessary to assure that the contractor provided services, documents, and material meet the prescribed requirements and to reject any or all services, documents, and material in a category when nonconformance is established.

3.3.2.3 Testing: The contractor shall develop and document test procedures, perform the tests and provide the results to the Government. The test procedures shall describe the proposed tests and inspections in sufficient depth to prove that equipment/system are thoroughly evaluated for conformance to the requirements of equipment/system specification(s). The contractor shall test for: Workmanship, all Environmental Factors, Maintainability, Reliability, Connectivity, Availability, Supportability, and Final Inspections, as defined in system/equipment specifications. The testing shall consider partitioning to enhance fault isolation, initialization of circuitry under test control, module interface for test access and control, circuit controllability and examination, test point placements, and Built In Test (BIT) fault isolation approach. The contractor shall submit the results of all the tests and inspections using the test procedures. The contractor shall perform the required calibration of any test equipment.

3.3.2.4 System Operation and Verification Test (SOVT):
The contractor shall develop and document a SOVT Planning and Execution Guide (SPEG) compliant SOVT package, perform the SOVT testing, and provide the results to the Government. The SOVT shall ensure satisfactory operation, availability and readiness after integration or installation. The contractor shall employ the following SOVT strategy: (1) System integration (in the laboratory environment) and equipment acceptance testing; (2) Baseline testing to assure the proper operating condition of all existing interfaces prior to any pre-installation activity and prior to dismantling or removal of existing connections or equipment; (3) Component in-place testing to verify that each component installed operates as demonstrated in the initial acceptance testing; (4) Bypass testing after equipment/system installation to

demonstrate that the shore is performing its designed function; (5) Test data interface exchange testing after installation of equipment/system to ensure that elemental test data can be exchanged between the components of the system; (6) Initial integration testing with operational programs loaded and program functions validated; and (7) Interoperability testing. All portions of the SOVT shall be witnessed by the Government representative specified in the task order. **(CDRL A004/A010)**

3.3.3 Interim Maintenance Support: The contractor shall provide on-site services for equipment/systems and perform troubleshooting, disassembly/assembly, modification, repair, and rebuild.

3.3.4 Verification and Validation (V&V): The contractor shall provide V&V support and develop V&V test documentation (test plans/procedures and reports or independent assessments); and test support. Other support shall include independent report of findings, identifying, recommending and correcting issues before and after test execution, and validating test results. The contractor shall use Government information resources such as SPAWAR Integrated Data Environment and Repository (SPIDER) and Configuration Canagement (CM) Professional (Pro) (CMPro). **(CDRL A010)**

3.3.5 Network User Pre-Migration, Migration, PC Refresh and PC Growth: The contractor shall develop network user pre-migration and migration support plans and procedures, PC Refresh/Growth plans and procedures, and shall support execution of migration and PC Refresh/Growth efforts. The contractor shall support Legacy Application data collection and rationalization, move user mailboxes and data, configure workstations, perform software and applications pushes, support customers and collect customer's surveys.

3.3.6 Provide a quarterly audit identifying HW, SW, and configuration differences between the modernizations, development and staging environments and include the audit report in the first Monthly Status Report following the audit. **(CDRL A001)**

3.3.7 Perform Pre-Installation and Test Check-Out (PITCO) & Bill of Materials (BOM) for all Government-procured and approved hardware to be utilized for engineering, deployment and upgrade efforts at OCONUS sites and within the NEN lab environment. **(CDRL A010)**

3.3.8 Maintain and update the service/solution/project BOM and include with the appropriate 405 document (2.0 Applicable Documents). The contractor shall ensure each BOM identifies all hardware, software, associated purchase costs, and assigned/deployed location (e.g. CONUS or OCONUS site, NEN Lab, etc.). The service or solution BOM will provide framework for new deployments (e.g. components, software, hardware, licenses, etc.) The BOM shall include functional and physical characteristics and specifications and a detailed cost breakout for each individual location, by room number.

3.4 **SYSTEM IMPLEMENTATION AND UPGRADE:** For the production engineering, installation of new capabilities and procurement of IT systems, the contractor shall:

3.4.1 Shore Implementation Support: The contractor shall perform Navy C4I shore based site system integration, deployment, troubleshooting, support SOVT execution and network configuration documentation updates, following SECNAVINST 5239.3C, DoDI 8500.01, and DoDI 8510.01. **(CDRL A004)**

3.4.2 Site Survey: The contractor shall support site visits, develop site in-brief and out-brief, draft site survey checklist, and report inclusive of implementation tasks, BoM, issues, security assessment, risk and recommendations.
Base Electronic Systems Engineering Plan (BESEP): The contractor shall develop a BESEP (Installation, Abbreviated, Guidance, Conceptual or for Military Construction), with upgrade detail provided to enable evaluation of operational impact (such as signal flow and site) on user activities.

3.4.3 Installation Design Plan (IDP) and As Built Drawings: The contractor shall develop, review and/or modify IDPs as required by the individual task order, Shore Installation Process Handbook Version 4.0 or latest version. Upon completion of the installation the contractor shall review changes to the design, per redlines, make changes to the IDP, and provide final version of the drawings as the final As Built as required. **(CDRL A004)**

3.4.4 Equipment and Material: The contractor shall generate, identify and verify material list or BoM, procure and deliver all equipment and incidental materials necessary to complete the site implementation/integration or upgrade.

3.5 **ENTERPRISE APPLICATION (EA) SUPPORT:** For the production engineering, installation of new capabilities and procurement of IT systems, the contractor shall:

The contractor shall deliver software capabilities required for effective command and control of warfighter and business missions by assuring compatibility with the networks Workstation Baseline and Security Configuration and protecting those capabilities by adhering to Office of the Chief of Naval Operations (OPNAV) security regulations.

3.5.1 Enterprise Application Analysis: The contractor shall evaluate proposed or candidate Commercial and Government Off-the-Shelf (COTS and GOTS) applications by ensuring the application is accredited by the Navy's Authorizing Official OPNAV Functional Area Manager (FAM) approval, and valid Secretary of the Navy last date allowed (SECNAV LDA), listed in the Department of the Navy Application and Database Management System (DADMS). In addition to an application's approval status in DADMS, networks that the application resides on must also be set as "Allowed" prior to the deployment on the designated network. Additional analysis includes at a minimum: customer software rationalization, licensing verification, version control, vendor maintenance or Program of Record (POR) support.

3.5.2 Enterprise Application Testing: The contractor will perform functional and security testing of Enterprise Applications prior to packaging an application for network deployment. Functional testing will ensure the Enterprise Application is at a minimum compliant/compatible with the current approved and accredited host workstation operating system (such as Windows 10), Group Policy Objects (GPO),

Navy Ports, Protocols, and Services Management (PPSM), and Workstation Baseline software and services.

3.5.3 Enterprise Application Packaging and Deployment: The contractor shall assess the software and develop a technical solution for deploying the software. The ideal solution is a single electronically deployable package and/or a hosted virtual application that can be deployed throughout the designated network. When either option is available, the contractor will develop local load installation procedures that can be easily understood and implemented in the field. The end result must adhere to specific Navy RMF standards and not present vulnerabilities that cannot be mitigated or remediated by an EA Security Engineer. For every application produced, applicable 400 level documentation will be developed to support deployment, installation and appropriate testing evaluation. **(CDRL A010)**

3.5.4 Enterprise Application Accreditation: The contractor shall provide Information Assurance (IA) support by scanning approved software with Assured Compliance Assessment Solution (ACAS), Security Content Automation Protocol (SCAP) tool, and Network Mapper (Nmap) and providing outputs of services and protocols. The contractor shall provide recommendations for technical documentation and systems improvement to the Security Assessment documentation and Enterprise Applications Process Guide. Assist with the Application Security Assessment (simple/complex assessment and Level Of Effort (LOE) determination by NAO Certification Agent and Validator) by ensuring applications are ready for an IA security review, working with vendor to resolve any initial findings as part of the IA security review, and working with the customer and applicable Program of Record (POR) to obtain any required documentation/information required. Ensure Federal Information Security Management Act (FISMA) compliancy of applications per the DODI 8500.2 and DIACAP policies. Review Security Technical Implementation Guides (STIGs) for Defense Information Systems Agency (DISA) and provide feedback to the Security Engineering and Certification & Accreditation Teams.

3.5.5 Enterprise Application Patch Management: Provide patch management support for all approved Enterprise Applications. The contractor shall provide support to the Government with timely deployment of patches, to meet the Joint Task Force-Global Networks Operations (JTF- GNO) deadlines, for patch deployment in accordance with Applicable Documents. Provide support to the Government in the preparation of standard biweekly activity reports and real-time Information Assurance Vulnerability Alert (IAVA) compliance reports, as required.

3.5.6 Enterprise Applications (EA) Information Center: The contractor shall develop or maintain a forward facing website that includes information about the status of Enterprise Application testing, network approval, customer service contact information, EA processes and other information that will support decisions by supporting Navy commands.

3.6 **WORKSTATION BASELINE SOFTWARE CONFIGURATION (WBSC) SUPPORT:** For the production engineering, installation of new capabilities and procurement of IT systems, the contractor shall:

The Contractor shall support the WBSC efforts. This requires the patching support for client operating systems as well as security patches. This task also includes the following efforts:

3.6.1 WBSC Support: The contractor shall provide engineering services to support Request for Change (RFC) process (in support of speed to capability for Navy networks). The contractor shall provide on-site ashore engineering subject matter expertise in support of ONE-NET services at overseas locations and at CONUS NIWC activities. The contractor shall provide engineering technical services to assist with system integration and site activation planning to include the formulation and tracking of delivery plans for equipment sub-systems to support contract requirements and its integration into NGEN. (CDRL A010)

3.6.2 WBSC Accreditation: The contractor shall provide Information Assurance analysis and scanning of new Workstation models and applications using Assured Compliance Assessment Solution (ACAS) and Security Compliance Automated Protocol (SCAP) or applicable security analysis tools and provide outputs of services and protocols. The Contractor shall assist the Application Security Assessment by ensuring that applications are ready for Information Assurance (IA) security compliance reviews. Contractor shall work with vendors to resolve any initial findings resulting from an IA security review. Contractor shall also work with customers to obtain any required documentation, media or installation instructions as required to process the RFC. The Contractor shall ensure that WBSC hardware and applications are in compliance with DODI 8500.2, policies and Federal Information Security Management Act (FISMA). The Contractor shall ensure compliance of Security Requirements Guides (SRG) or Security Technical Implementation Guides (STIGs) for Defense Information Systems Agency (DISA) and provide feedback to the Security Engineering and Certification & Accreditation (C&A) Teams.

3.6.3 WBSC Patch Management: The Contractor shall provide Patch Management for all approved baseline workstation (Line of business) applications. The Contractor shall support the Engineering team to incorporate patches into the patch management system. This effort will support deficiency correction and modification for the WBSC Software Packages that will be deployed at eight separate environments (2 lab and 6 operational), as patches are released. Duties include testing patches (manually and via automated methods) in the lab environment and documentation of patches that apply to a particular WBSC image version. The contractor shall provide assistance with issues regarding patch deployment to the operational sites during modernization efforts.

*Begin O&M,N Sections*

3.7 **INTEGRATED PROJECT TEAM and PROJECT MANAGEMENT SUPPORT:**
For the sustainment and maintenance of fielded IT systems, the contractor shall:

3.7.1 Task Status Reports: For each task the contractor shall provide monthly progress and status reports. This report shall include reconcilable expenditure reports that shall track back to the initial quotation. **(CDRL A001)**

3.7.2 Management Reviews: The contractor shall provide project management support for the task orders issued under this contract and participate in and support program reviews held by NIWC Systems Pacific (NIWC PAC). This support shall include generating meeting minutes, identifying and tracking outstanding actions, management documentation, such as a Project Management Plan, Project-Level Integrated Master Schedule (IMS), Work Breakdown Structure (WBS) and individual Plan of Action and Milestones (POA&M), development/updates and all other matters to ensure the successful execution of all work to be performed on the task orders. **(CDRL A008/A009)**

3.7.3 Work with IPT lead and members to identify and prioritize tasks for the team; review progress; participate in meetings; review, track and process action items; and provide production engineering assessments and technical verification and validation of the capabilities and deficiencies of the systems and vendors.

3.7.4 Assess current and future system and software project requirements, analyze changes and situations and develop, and propose or recommend tentative approaches and solutions using a variety of tools, techniques, or processes.

3.7.5 Provide input for the preparation and presentation of briefing material and development of various program, system and business development documents.

3.7.6 Assess progress and identify schedule and technical variances and provide milestone support for major project efforts and facilitate and document project team activities. Documentation produced or modified shall be in the appropriate format and maintained in the electronic folders resident on the local area network. **(CDRL A001)**

3.7.7 Provide meeting minutes and an action item tracker for all meetings led by the contractor or in which the contractor attends in a supporting role. The contractor shall consolidate all action item data in a central location on a NEN collaboration tool. **(CDRL A009)**

3.7.8 Conduct technical, cost, and schedule risk assessments.

3.8 **SUSTAINMENT ENGINEERING SUPPORT:** For the sustainment and maintenance of fielded IT systems, the contractor shall:

3.8.1 Technical Support: The contractor shall conduct and/or participate in technical reviews. The contractor shall coordinate meetings, developing agenda items, participate in meetings, generate minutes, and track action items as required. The contractor shall develop and/or revise the following documentation; Request for Change (RFC), Specification Change Notices (SCN), Engineering Change Request (ECR), Engineering Change Notice (ECN), Fleet Readiness Certification Board (FRCB), and Field Changes (FCs). The contractor shall coordinate, attend and participate in site surveys, installations, implementations, technical assistance, meetings and conferences, and exchange information with program managers, engineers and users. The contractor shall support customers worldwide in different time zones and attend meeting at different times to support program requirements. **(CDRL A001/A009)**

3.8.2 System Evaluations and Trade Study Support: The contractor shall perform system evaluations/analysis, requirement reviews, Technology Readiness Level (TRL)

Analysis, product evaluations, risk analysis, security evaluations and analysis to include Certification Test and Evaluations (CT&E) and Site Test and Evaluation (ST&E), decision papers, business case analysis or trade studies to determine where changes might be recommended to correct deficiencies, new product recommendation, achieve cost savings or improve operations and maintenance.

3.8.3 Design Analysis Support: The contractor shall provide plans, design analysis and recommendations for the following: Information Systems, Certification and Accreditation (C&A) Safety; Human Factors; Reliability, Maintainability, Availability, Heating/Cooling; Control of electrostatic discharge and Mercury contamination; and Power or Power Distribution.

3.8.4 Mockup Support: The contractor shall develop, document, validate, and maintain engineering mockups for specific system/equipment in accordance with specific system/equipment specification(s).

3.8.5 Engineering Development Model (EDM) Support: The contractor shall develop, document, validate, test and deliver EDMs for IT systems or equipment in accordance with specific system/equipment specification(s). EDM development shall identify operational and security configuration, integration, deployment and life cycle support equipment requirements.

3.8.6 Engineering Information Bulletins/Article(s) Support: The contractor shall develop and prepare periodic articles for inclusion into Newsletter(s), Standard Operating Procedures (SOPs) and Engineering Information Bulletins.

3.8.7 Drawing Support: The contractor shall develop drawing packages using existing packages to the maximum extent. The contractor shall develop, validate, modify, maintain, and utilize drawing packages, drawing trees (interrelationship of engineering drawings and associated lists), "As-Built" drawings, red-lined drawings, Installation Control Drawings (ICD), Installation Design Plans (IDP) and block diagrams (schematic and functional, including all interfaces) using computer aided design software compatible with existing formats.

3.8.8 Mission Critical Computer Resources (MCCR) Support: The contractor shall develop, procure, document, test, and maintain any required MCCR and computer resources support.

3.8.9 Systems Support: The contractor shall provide support in developing, maintaining, documenting, integrating, and installing upgrades to shore systems that enables voice, video and data transmissions from any PC throughout the Navy. This will allow warfighters to exchange classified, unclassified, tactical or non-tactical information. The contractor shall develop, modify, operate, test, implement, document, and maintain Automated Information Systems (AIS). The contractor shall provide AIS services on a variety of systems and specialized workstations (i.e. computer-aided design) to include the following: (1) entry of data; (2) extracting, interpreting, editing and consolidating data; (3) designing, setting-up and implementing special input formats; (4) transmitting and receiving data; (5) documenting procedures for inputting data; (6) controlling the receipt and transmission of data; (7) specification of outputs; (8) operation of information system equipment; (9) design, implementation and management of databases; and (10) security. The contractor shall provide networking services that support the transfer of data, video, imagery and multimedia. The

contractor shall provide the capability to manage network objects such as host computers, routers, local area networks, and wide area networks.

3.8.10 Rapid Prototyping Support/New Developmental Item: The contractor shall provide rapid prototyping support between new designs and modernization. This shall include the engineering, integration, documentation, and fabrication of enough subassemblies and assemblies that constitute either parts of or an entire system/suite as required to support the design validation and documentation verification and validation processes prior to full modernization. **(CDRL A004)**

3.8.11 Network Response Group (NRG): The contractor shall provide a NRG as necessary to support a limited rapid response to specific fleet technical assistance requirements. This response shall include the capability to diagnose and repair the complete network, end-to-end. This shall include, at a minimum, the computer networks, fiber optics, microwave, baseband, and all interconnections of the system network.

3.8.12 Network Systems Engineering: The contractor shall provide systems engineering support in the form of the development of technical insertions and solutions to supported systems. This support shall include; development and review of 400 series documents (High Level Architecture, Detailed Design, Requirements and Configuration Settings, Installation Procedures, Test Plans, Test Reports), Engineering Change Order (ECO), Bill of Materials (BoM), Operations Guidelines, Operations Procedures, Request for Changes (RFCs) and other technical documentation as required. Develop and review design, technical reports, cost estimates, and correspondence including letters and messages. Prepare and review design proposals, security documents, verify Installation Design Plans (IDPs)/drawings, and ensure specifications and design meet performance requirements. **(CDRL A003/A004)**

3.8.13 Prepare report(s), which include success criteria for installations, lessons learned/best practices, and improvement of fielded subsystems in terms of operability, technical merit, and schedule risks. **(CDRL A007)**

3.8.14 Create, modify, and/or update specifications and interface documentation to describe the physical, functional, and performance interfaces; and hardware, software, and system-level performance requirements. Documentation of information systems shall include preparing or updating system engineering plans (SEP), technical manual, operation and maintenance manuals, style guides, test plans, test reports, implementation plans, recommendations, bulletins, outlines and white papers in accordance with NEN standards. **(CDRL A006)**

3.9 **TECHNICAL SUPPORT:** For the sustainment and maintenance of fielded IT systems, the contractor shall:

3.9.1 Technical Assistance Site Support: The contractor shall provide site support to determine the root cause of technical issues affecting system performance. The contractor shall coordinate with Government site personnel during the execution of the requirement. The contractor shall provide recommendations, correct issues, verify correction, document changes in relevant and applicable system configuration documents, and provide a final trip report documenting analysis, findings, corrected

action, site points-of- contact, required documentation changes, and changes to applicable network devises. The contractor shall provide on-call 24/7 support (via telephone, chat or e-mail) and on-site (travel) services on equipment/systems to perform troubleshooting, correct CASREPs, provide Tier IV assistance, checkout, repair, and test worldwide. **(CDRL A003)**

3.9.2 Quality Assurance and Testing:

3.9.2.1 Quality Assurance (QA) Program: The contractor shall provide and maintain a quality/inspection system that, as a minimum, adheres to the requirements of ISO 9001:2008 or equivalent and supplemental requirements imposed by this contract. ISO 9001:2008 registration and certification will be considered as one method of proof of compliance with this requirement.

The quality system shall be documented and contain procedures, planning, and all other documentation and data necessary to provide an efficient and effective quality system based on their internal auditing system. The quality system shall be made available to the Government for review during predetermined visits. Existing quality documents that meet the requirements of this contract may continue to be used. The Government reserves the right to witness any specified inspections, installations, demonstrations, tests, validations, and verifications. The Government reserves the right to disapprove the contractor's and/or subcontractor's quality system or portions thereof when the quality system(s) fails to meet contractual requirements at either the program or worksite services level. The documented quality assurance system shall be used to ensure that the end product of each task conforms to contract requirements whether produced by the contractor or provided by approved subcontractors or vendors. The quality assurance system shall provide for control over all phases of the various types of tasks, from initial manning and material ordering to completion of final tasking, before offering to the Government for acceptance as specified in this task order/SOW. All services shall be rendered according to the documented quality system and directly supervised by individuals qualified in the relevant profession or trade. **(CDRL A004)**

3.9.2.2 Quality Control: Unless otherwise directed, the contractor is responsible for all quality control inspections necessary in the performance of the various tasks as assigned and identified by the respective Work Breakdown Structure (WBS), POA&M or procedural quality system document. The Government reserves the right to perform any inspections deemed necessary to assure that the contractor provided services, documents, and material meet the prescribed requirements and to reject any or all services, documents, and material in a category when nonconformance is established.

3.9.2.3 Testing: The contractor shall develop and document test procedures, perform the tests and provide the results to the Government. The test procedures shall

describe the proposed tests and inspections in sufficient depth to prove that equipment/system are thoroughly evaluated for conformance to the requirements of equipment/system specification(s). The contractor shall test for: Workmanship, all Environmental Factors, Maintainability, Reliability, Connectivity, Availability, Supportability, and Final Inspections, as defined in system/equipment specifications. The testing shall consider partitioning to enhance fault isolation, initialization of circuitry under test control, module interface for test access and control, circuit controllability and examination, test point placements, and Built In Test (BIT) fault isolation approach. The contractor shall submit the results of all the tests and inspections using the test procedures. The contractor shall perform the required calibration of any test equipment.

3.9.2.4 System Operation and Verification Test (SOVT):
The contractor shall develop and document a SOVT Planning and Execution Guide (SPEG) compliant SOVT package, perform the SOVT testing, and provide the results to the Government. The SOVT shall ensure satisfactory operation, availability and readiness after integration or installation. The contractor shall employ the following SOVT strategy: (1) System integration (in the laboratory environment) and equipment acceptance testing; (2) Baseline testing to assure the proper operating condition of all existing interfaces prior to any pre-installation activity and prior to dismantling or removal of existing connections or equipment; (3) Component in-place testing to verify that each component installed operates as demonstrated in the initial acceptance testing; (4) Bypass testing after equipment/system installation to demonstrate that the shore is performing its designed function; (5) Test data interface exchange testing after installation of equipment/system to ensure that elemental test data can be exchanged between the components of the system; (6) Initial integration testing with operational programs loaded and program functions validated; and (7) Interoperability testing. All portions of the SOVT shall be witnessed by the Government representative specified in the task order. **(CDRL A004/A010)**

3.9.3 Interim Maintenance Support: The contractor shall provide on-site services for equipment/systems and perform troubleshooting, disassembly/assembly, modification, repair, and rebuild.

3.9.4 Verification and Validation (V&V): The contractor shall provide V&V support and develop V&V test documentation (test plans/procedures and reports or independent assessments); and test support. Other support shall include independent report of findings, identifying, recommending and correcting issues before and after test execution, and validating test results. The contractor shall use Government information resources such as SPAWAR Integrated Data Environment and Repository (SPIDER) and Configuration Canagement (CM) Professional (Pro) (CMPro). **(CDRL A010)**

3.9.5 Network User Pre-Migration, Migration, PC Refresh and PC Growth: The contractor shall develop network user pre-migration and migration support plans and procedures, PC Refresh/Growth plans and procedures, and shall support execution of migration and PC Refresh/Growth efforts. The contractor shall support Legacy Application data collection and rationalization, move user mailboxes and data, configure workstations, perform software and applications pushes, support customers and collect customer's surveys.

3.9.6 Provide a quarterly audit identifying HW, SW, and configuration differences between the modernizations, development and staging environments and include the audit report in the first Monthly Status Report following the audit. **(CDRL A001)**

3.9.7 Perform Pre-Installation and Test Check-Out (PITCO) & Bill of Materials (BOM) for all Government-procured and approved hardware to be utilized for engineering, deployment and upgrade efforts at OCONUS sites and within the NEN lab environment. **(CDRL A010)**

3.9.8 Maintain and update the service/solution/project BOM and include with the appropriate 405 document (2.0 Applicable Documents). The contractor shall ensure each BOM identifies all hardware, software, associated purchase costs, and assigned/deployed location (e.g. CONUS or OCONUS site, NEN Lab, etc.). The service or solution BOM will provide framework for new deployments (e.g. components, software, hardware, licenses, etc.) The BOM shall include functional and physical characteristics and specifications and a detailed cost breakout for each individual location, by room number.

3.10 **INTEGRATED LOGISTICS SUPPORT (ILS):** For the sustainment and maintenance of fielded IT systems, the contractor shall:

3.10.1 ILS Planning and Life Cycle Support:

3.10.1.1 Integrated Logistics Support (ILS) Planning: The contractor shall develop and maintain Integrated Logistics Support Plan(s) (ILSP); User's Logistics Support Summary(s) (ULSS); Logistics Requirements and Funding Summary(s) (LRFS); Logistics Support Analysis Plan(s) (LSAP); Computer Resources Integrated Support Document (CRISD) and life cycle cost estimating. The impacts on all ILS elements shall be discussed in all ILS Plans, system engineering analyses and engineering change proposals. The ILS elements include the following: (1) Technical data; (2) Training and training support; (3) Maintenance; (4) Supply support; (5) Configuration management; (6) Support equipment; (7) Manpower and personnel; (8) Packaging, handling, storage and transportation; (9) Computer resources support; (10) Facilities; and (11) Design interface.

3.10.1.2 Logistic Support Analysis (LSA): The contractor shall perform LSA supportability analyses of systems/ equipment. The LSA process is iterative and may be continued through the life cycle of the systems/equipment to address engineering changes. These analyses shall include at a minimum: (1) identification of hardware or software for which the Government will not or

may not receive full rights due to constraints imposed by regulations or laws limiting the information that must be furnished because of proprietary or other source control considerations;
(2) development of supportability, cost, and readiness objectives including risk assessment; and
(3) development of supportability and supportability related design constraints for inclusion in specification(s) and other requirement documents.

3.10.2 Technical Data Support:

3.10.2.1 Technical Publication Support: The contractor shall develop and validate Type II equipment technical manuals, Type III system technical manuals and technical manual supplements to support operation and maintenance at all three maintenance levels. When required, the contractor shall procure commercial manuals for fleet and training support.

3.10.2.2 Technical manual (military and commercial) requirements and deficiencies shall be identified as part of the LSA supportability evaluation. The contractor shall develop and validate the Illustrated Parts Breakdowns and Maintenance Standards Books. **(CDRL A006)**

3.10.3 Training Support:

3.10.3.1 Formal Training: The contractor shall develop formal training for both the organizational level and maintenance level, and training rosters. All course material required for instruction (i.e. curriculum, training audiovisual aids, outlines and guides) for any course shall be developed and validated by the contractor. At a minimum, the course content shall provide personnel with the following: Uses; Interfaces; Theory of operation; Synopsis of the equipment and equipment checkout; Startup procedures; Operation and shutdown safety procedures; Procedures for Alignment, Inspections, and maintenance; Assembly/disassembly; Troubleshooting; Use of tools and test equipment; and Replacement of parts and repair in accordance with the maintenance concept of the equipment/system. Developed courses shall provide work experience with the equipment/system, to include preventive and corrective maintenance procedures. **(CDRL A011/A012)**

The contractor shall participate in administrative tasks such as scheduling classes, tracking student loading and instructor assignments, and processing payments, receipts and invoices. The contractor shall provide Government with analysis and metrics relating to training effectiveness based on trainee feedback, instructor observations, and stakeholder reviews.

3.10.3.2 On-the-Job Training (OJT) and Handbook Development. The contractor shall develop and conduct job skills-type training (organization and maintenance) for system/equipment following system/equipment upgrade. The training shall provide personnel with a synopsis of what the formal training covers as discussed in 3.4.3.1 above.

3.10.4 Supply Support: The contractor shall develop specific Provisioning Technical Documentation (PTD). Provisioning information shall be developed and delivered using the Interactive Computer-Aided Provisioning System (ICAPS) or other Government-approved Automated Data Processing (ADP) capability. The contractor shall submit Design Change Notices (DCN) to identify changes to Provisioning Technical Documentation (PTD). Provisioning screening and technical information coding (including replacement factors; mission essentiality; and source, maintenance and recoverability codes) shall be provided for each item listed on the Provisioning Parts List (PPL). The contractor shall develop, compute and document Program Support Data (PSD) on Forms NAVSUP 1390 (HSC End Item Program Support Data), NAVSUP 1390/1 (Equipment Installation Data, and NAVSUP 1392 (HSC Secondary Item Funding Requirements) using the Navy's authorized ADP capability called, "Parts Reporting and Tracking System (PARTS)". The contractor shall request/confirm Government nomenclature; request assignment of serial numbers, request assignment of national stock numbers; and provide identification plates.

3.11 **CONFIGURATION MANAGEMENT:** For the sustainment and maintenance of fielded IT systems, the contractor shall:

3.11.1 Configuration Support: The contractor shall develop, implement and maintain a configuration management program, including configuration audit plans, covering hardware and software in an integrated approach. The contractor shall verify and maintain complete and accurate configuration identification of each Configuration Item (CI)/Computer Software Configuration Item (CSCI) and Government-approved established Functional, Allocated, and Product baselines for equipment/systems.

3.11.2 Baseline Documents: The contractor shall draft and update baseline documents (e.g. system concept, system configuration, specifications, reports, accreditation documents, Logical Network Diagrams (LNDs), SOPs, drawings and associated lists, manufacturing processes and procedures, test and inspection plans/procedures, quality assurance provisions, inspection and test equipment requirements, packaging requirements, software documentation, technical manuals, maintenance and supply support documentation, and training/training support documentation) and CI/CSCI as a result of an approved Engineering Change Proposal (ECP), RFC, Request for Deviation, or Request for Waiver. The Configuration Data Managers Database-Open Architecture (CDMD-OA) shall be developed and provided to the fleet.

3.11.3 Configuration Status Accounting: The contractor shall provide configuration status accounting, which shall delineate the status of changes from the baseline, the status of proposed changes, and the status of implementation of approved changes. The contractor may use the Government-approved ADP system(s) (such as CMPro) for configuration status accounting. **(CDRL A003)**

3.12 **TIER IV OCONUS SUPPORT:** For the sustainment and maintenance of fielded IT systems, the contractor shall:

3.12.1 The Contractor shall provide Tier IV (fault tolerant site infrastructure) technical support to both Fleet and NIWC Enterprise customers in support of ONE-NET networks and applications as requested by the government.

3.12.2 The Contractor shall also provide engineering services to support the ONE-NET Request For Change (RFC) process (in support of speed to capability for Navy networks). ONE-NET speed to capability efforts will be as directed by ISEA in support of Fleet and NIWC Enterprise objectives. The Contractor will provide on-site ashore engineering subject matter expertise in support of ONE-NET services at overseas locations listed in section 3.0 and at CONUS NIWC activities.

3.12.3 The Contractor will provide engineering technical services to assist with system integration and site activation planning to include the formulation and tracking of delivery plans for equipment sub-systems to support ONE-NET requirements and it's integration into Navy Next Generation Enterprise Networks (NGEN). (CDRL A006)

3.12.4 The Contractor will assist the customer with installing and integrating ONE-NET systems to replace legacy networks in support of three OCONUS Theater Network Operations and Security Centers (TNOSCs) at Naval Computer and Telecommunications Station (NCTS) Naples, NCTS Bahrain and NCTS Far East (at Yokosuka, Japan) and outlying Navy ports/stations as required.

3.12.5 The Contractor shall provide SME services to assist with preparation and analysis of integration designs, implementation concepts and systems to include reviewing and assisting in the reduction of program risk per applicable risk management plans. The Contractor will assist enterprise program offices and Fleet customers with the employment of technical solutions associated with the NGEN and ONE-NET "Deployable-Embarkable" project and concurrent safeguarding of approved Navy network security directives. The potential for domestic and overseas travel as well as short deployment periods on Navy platforms exists. (Amendment 1) Classification of systems supported includes UNCLASSIFIED, CONFIDENTIAL and SECRET (to include CENTRIXS Coalition).

3.12.6 The contractor shall provide on-call 24/7 support (via telephone, chat or e-mail) and on-site (travel) services on equipment/systems to perform troubleshooting, correct Casualty Reports (CASREPs), provide Tier IV assistance, checkout, repair, and test worldwide.

## 4.0 DATA DELIVERABLES:

Data deliverables shall be reviewed IAW "DON Policy on Digital Product/Technical Data, ASN RD&A memo of 23 OCT 2004". Technical data and computer software delivery requirements will be specified through use of a Contract Data Requirements List, DD Form 1423, at the individual task order level. To ensure information compatibility, the contractor shall guarantee all deliverables (i.e., CDRLs), data, and any other required correspondence are provided in a format approved by the receiving government representative.

**5.0 SECURITY:**

The nature of this effort requires access to Secret information. The work performed by the contractor will include access to unclassified and up to Secret for data and information. Contractor personnel working at Government facilities must have a minimum level of a Secret Clearance in accordance with DD Form 254, Contract Security Classification Specification for access to classified equipment, and/or spaces. The contractor will be required to attend meetings classified up to Secret level. The Contractor will require access to Communications Security and Secure Internet Protocol Router Network (SIPRNet).

Although no access to North Atlantic Treaty Organization (NATO) information is needed under this contract, some employees designated as Limited System Administrators on computer systems accredited to process up to NATO Secret data may come into contact with NATO classified data. Limited Privilege System Administrators shall have a final Secret clearance (this is when an individual can change passwords, but is not able to rewrite files), see DD254, Contract Security Classification Specification for additional information.

Some contractors will only need to receive the NATO awareness brief and complete the derivative classification training prior to accessing SIPRnet; training is to be provided by the prime contractor's facility security officer, see DD254, Contract Security Classification Specification for additional information.

Contractors that access Navy IT are also required to follow the provisions contained in DON CIO Memorandum: Acceptable Use of Department of the Navy Information Technology (IT).

As required by National Industrial Security Program Operating Manual (NISPOM) Chapter 1, Section 3, contractors are required to report certain events that have an impact on: 1) the status of the facility clearance (FCL), 2) the status of an employee's personnel clearance (PCL); may indicate the employee poses an insider threat the proper, 3) the proper safeguarding of classified information, and 4) or an indication that classified information has been lost or compromised. Contractors working under NIWC Pacific contracts will ensure information pertaining to assigned contractor personnel are reported to the Contracting Officer Representative (COR)/Technical Point of Contact (TPOC), the Contracting Specialist, and the Security's COR in addition to notifying appropriate agencies such as Cognizant Security Agency (CSA), Cognizant Security Office (CSO), or Department Of Defense Central Adjudication Facility (DODCAF) when that information relates to the denial, suspension, or revocation of a security clearance of any assigned personnel; any adverse information on an assigned employee's continued suitability for continued access to classified access; any instance of loss or compromise, or suspected loss or compromise, of classified information; actual, probable or possible espionage, sabotage, or subversive information; or any other circumstances of a security nature that would affect the contractor's operation while working under NIWC Pacific contracts.

If foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted to the Commanding Officer, Attn: Foreign Travel Team, Naval Information

Warfare Center Pacific, 53560 Hull Street Building 27, 2nd Floor -Room 206, San Diego, CA 92152 for action. A Request for Foreign Travel form shall be submitted for each traveler, in advance of the travel, to initiate the release of a clearance message at least 30 days in advance of departure. Each Traveler must also submit a Personal Protection Plan and have a Level 1 Antiterrorism/Force Protection briefing within one year of departure and a country specific briefing within 90 days of departure. Anti-Terrorism/Force Protection (AT/FP) briefings are required for all personnel (Military, DOD Civilian, and contractor) per OPNAVINST F3300.53C. Contractor employees must receive the AT/FP briefing annually. The briefing is available at Joint Knowledge Online (JKO): https://jkodirect.jten.mil (prefix): JS; course number: US007; title: Level 1 Anti-terrorism awareness training, if experiencing problems accessing this website contact the JKO Help Desk (24 hours a day/7 days a week, jkohelpdesk@jten.mil, 757-203-5654). Sere 100.2 Level A code of conduct training is also required prior to OCONUS travel for all personnel. Sere 100.2 Level A training can be accessed at http://jko.jfcom.mil (recommended), https://jkodirect.jten.mil/atlas2/faces/page/login/login.seam, recommend course: prefix: J3T: course #: A-US1329, for civilian, military, and contractors. Personnel utilizing the JKO site must have a CAC or contractor shall request a sponsored account to access the training. Other specialized training for specific locations may also be required contact the NIWC Pacific foreign travel team.

Contractors working in the CENTCOM AOR are bound by the provisions of DFARS 252.225. - 7995 (contractor personnel performing in the CENTCOM AOR). Additional information can be found on the DCAA website, http://dcaa.mil/dfars.html.

Finally, EUCOM has mandated that all personnel going on official travel to the EUCOM AOR must now register with the Smart Traveler Enrollment Program (STEP). When you sign up, you will automatically receive the most current information the State Department compiles about your destination country. You will also receive updates, including Travel Warnings and Travel Alerts. Sign up is one-time only, after you have established your STEP account, you can easily add official or personal travel to anywhere in the world, not just EUCOM. http://travel.state.gov/content/passports/en/go/step.html

5.1 **OPERATIONS SECURITY:**

OPSEC is a five step analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; develop countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce or process Critical Information or CPI, and therefore all Contractor personnel must practice OPSEC. All work is to be performed in accordance with DoD OPSEC requirements, and in accordance with the OPSEC attachment to the DD254.

5.1.1 Operations Security (OPSEC) Requirements: Security programs are oriented towards protection of classified information and material. Operations Security (OPSEC) is an operations function, which involves the protection of any critical information –

focusing on unclassified information that may be susceptible to adversary exploitation. Pursuant to DoDD 5205.02E SECNAVINST 3070.2A, and NAVWARINST 3432.1, NAVWAR/NIWC Atlantic/NIWC Pacific's OPSEC program implements requirements in DoD 5205.02-M – OPSEC Program Manual. Note: OPSEC requirements are applicable when contract personnel have access to classified information, unclassified Critical Program Information (CPI), Controlled Unclassified Information (CUI) or Department of Navy (DoN) networks.

5.1.2 Local and Internal OPSEC Requirement: Contractor personnel, including subcontractors if applicable, shall adhere to the OPSEC program policies and practices as cited in the NAVWARINST 3432.1 and existing local site OPSEC procedures. The Contractor shall development their own internal OPSEC program specific to the contract and based on NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC requirements. The Contractor's program shall identify the current contractor site OPSEC Officer/Coordinator/POC.

5.1.3 OPSEC Training: Contractor shall track and ensure applicable personnel receive initial and annual OPSEC awareness training. Training may be provided by the government or by the contractor's OPSEC Manager. Contractor training shall include, at a minimum, cover OPSEC as it relates to contract work; discuss the Critical Information applicable in the contract; applicable review of government Critical Information and Indicators List(s) (CIIL); social media awareness and vulnerabilities; local threats; how to protect, transmit, and destroy controlled unclassified information; risks and guidance pertaining to geolocation-capable devices, applications, and services; and OPSEC review procedures for public release. The Contractor shall ensure that training materials developed by the Contractor shall be reviewed by the NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC Officer, who will ensure it is consistent with NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC policies. OPSEC training requirements are applicable for personnel during their entire term supporting NAVWAR/NIWC Atlantic/NIWC Pacific contracts and for the duration of DoN network access.

5.1.4 NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC Program: If required, the Contractor shall participate in NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC program briefings and working meetings, and complete any required OPSEC survey or data call within the timeframe specified.

5.2 **TRUSTWORTHINESS INVESTIGATIONS:**

This applies to contractor personnel who do not require a clearance and will only work on unclassified data. See definitions below.

6.2.2.1 Tier 3/3R: IT-II Position (Limited Privileged)

Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the IT-I category, includes but is not limited to:

- Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;

- Accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than $10 million per year. Other positions are designated by Naval Information Warfare Center, Pacific (NIWC Pacific) that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in IT- I positions. Personnel whose duties meet the criteria for an IT-II Position require a favorably adjudicated National Agency Check with Local Agency Check and Credit Check (NACLC) or Tier 3/3R.

5.3 **Tier 1/1R: IT-III Position (Non-Privileged)**

- All other positions involving Federal IT activities. Incumbent in this position has non-privileged access to one or more DoD information systems, application, or database to which they are authorized access. Personnel whose duties meet the criteria for an IT-III Position designation require a favorably adjudicated National Agency Check with Inquiries (NACI) or Tier 1/1R.

## 6.0 INFORMATION ASSURANCE WORKFORCE (IAWF) CERTIFICATION REQUIREMENT:

6.1 **Cyber Security Workforce (CSWF):**

In accordance with DFARS Subpart 5239.71, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, the contractor performing Information Assurance (IA) functions that are designated as Cyber Security Workforce (CSWF) positions in accordance with DoD 8570.01-M Information Assurance Workforce Improvement Program shall be trained and certified in accordance with DFARS Clause 252.239-7001, Information Assurance Contractor Training and Certification (IACT&C), and DoD 8570.01-M Series prior to accessing DoD information systems.

6.1.1 IAT Level I and Level II CSWF certifications will be required and maintain current, all training, certification, and qualifications for engineering and technical personnel working directly with the networks. **(CDRL A002)**

## 7.0 REPORTING REQUIREMENTS FOR CONTRACTED SERVICES:

See Services Contract Reporting (SCR) requirements in the SOW Addendum.

## 8.0 SPECIAL ACCOMMODATIONS:

The Government will provide access to Government workspaces, but any special accommodation requests (such as ergonomic chairs, “standing” desks etc.) shall be the responsibility of the contractor to provide for its employees.

8.1 **MOTOR VEHICLES:**

The contractor may use Government vehicles as authorized in the performance of specific task orders. The contactor must be properly insured for vehicles (Government or contractor owned/rented) operated in connection with the task orders. The contractor shall provide a certificate of insurance coverage to the contracting officer verifying it has the proper insurance to operate the vehicles.

8.1.1 Contractor shall verify the driving requirements for each installation site and comply with the requirements. Contractor shall coordinate with installation sites located in foreign countries to obtain international driver's license prior to travel.

8.1.2 Contractor shall provide rigging, forklift, crane service, and other services required to accomplish equipment installation/removal/relocation and personnel transport. The contractor shall provide operators with proper licenses to operate aforementioned services. Contractors performing material handling operations must be trained licensed and possess a valid medical examiner's certificate.

8.2 **GFM/GFE:**

A listing of Government Furnished Material (GFM) or Government Furnished Equipment (GFE) will be specified in each task order. All GFM/GFE furnished during the life of the contract remains the property of the Government, and if removed from NIWC Pacific shall be returned upon completion of the tasking unless otherwise specified in the individual task order.

8.3 **TRAVEL**:

The following long distance travel is estimated for the performance of this task:

| From | To | Number of Trips | Number of People | Number of Days |
|---|---|---|---|---|
| San Diego, CA | Washington, D.C. | 40 | 5 | 10 |
| San Diego, CA | Manama, Bahrain/ Jebel Ali | 120 | 20 | 68 |
| San Diego, CA | Yokosuka, Japan | 120 | 20 | 68 |
| San Diego, CA | Atsugi/Iwakuni | 45 | 19 | 54 |
| San Diego, CA | Misawa | 45 | 19 | 54 |
| San Diego, CA | Okinawa | 45 | 19 | 54 |
| San Diego, CA | Guam | 45 | 19 | 54 |
| San Diego, CA | Sasebo | 45 | 19 | 54 |
| San Diego, CA | Korea | 45 | 19 | 54 |
| San Diego, CA | Diego Garcia | 40 | 5 | 28 |
| San Diego, CA | Singapore | 45 | 19 | 54 |
| San Diego, CA | Naples, Italy | 120 | 20 | 68 |
| San Diego, CA | Sigonella | 45 | 19 | 54 |
| San Diego, CA | Rota | 45 | 19 | 54 |
| San Diego, CA | Souda Bay | 45 | 19 | 54 |

If foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted for action to:

Commanding Officer
Attn: Foreign Travel Team, Naval Information Warfare Center Pacific (NIWC Pacific)
53560 Hull Street

Building 27, 2nd Floor -Room 206
San Diego, CA 92152

Each Traveler must comply with the following:

(1) Request for Foreign Travel form – shall be submitted for each traveler, in advance of the travel, to initiate the release of a clearance message at least 30 days in advance of departure.
(2) Personal Protection Plan
(3) Level 1 Antiterrorism/Force Protection (AT/FP) – briefing is required within one year of departure and a country specific briefing within 90 days of departure.
    a) AT/FP briefings are required for all personnel (Military, DOD Civilian, and contractor) per Office of the Chief of Naval Operations Instruction (OPNAVINST) F3300.53C.
    b) Contractor employees must receive the AT/FP briefing annually.
    c) The briefing can be accessed at:
        i) Joint Knowledge Online (JKO): https://jkodirect.jten.mil
        ii) Course number: US007
        iii) Title: Level 1 Anti-terrorism Awareness Training
        iv) If experiencing problems accessing this website, contact JKO Help Desk (24 hours a day/7 days a week, jkohelpdesk@jten.mil, 757-203-5654)
(4) Survival, Evasion, Resistance, and Escape (SERE) 100.2 Level A –
    a) Training can be accessed at:
        i) http://jko.jfcom.mil (recommended), https://jkodirect.jten.mil/Atlas2/page/desktop/DesktopHome.jsf
        ii) Prefix: J3T
        iii) Course #: A-US1329
        iv) Personnel utilizing this site must have a CAC or contractor shall request a sponsored account to access the training.
(5) Specialized training for specific locations, such as SOUTHCOM human rights, or US forces Korea entry training, may also be required; NIWC Pacific security personnel will inform you if there are additional training requirements.
(6) EUCOM has mandated that all personnel going on official travel to the EUCOM AOR must now register with the Smart Traveler Enrollment Program (STEP). This site can be accessed at: http://travel.state.gov/content/passports/en/go/step.html.

***Contractor Notification – Awareness of Expectations***

Contractor personnel are reminded of their obligation to safeguard the vital relationship our Nation has with Foreign Countries. This includes personal conduct while performing under the contract and on one's personal time because, at all times, you are viewed by our partners as a representative of the United States, our Navy, and NAVWAR. Therefore, professional, courteous, and culturally aware conduct is necessary at all times. Inappropriate conduct, and especially intoxication and criminal behaviors, will not be tolerated. An all too common nexus for personnel misconduct while on travel is irresponsible consumption of alcohol. Intoxication increases your vulnerability to crime, injury, arrest, terrorism and espionage.

While traveling on official business, representing and performing in support of NAVWAR's mission, all personnel, including military, civilian and contractors, are expected to act in a professional and responsible manner. In order to promote effective relationships with business partners and allied nations, it is incumbent on contractor personnel to follow local laws and employ courteous and culturally aware behavior. Inappropriate conduct may jeopardize important relationships for the United States Navy, NAVWAR, NIWC Pacific and NIWC Atlantic, and will not be tolerated.

In all cases, Contractors are reminded of their responsibilities under FAR 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015). The clause requires the contractor to:

- Have a written code of business ethics and conduct;
- Make a copy of the code available to each employee;
- Exercise due diligence to prevent and detect criminal conduct;
- Promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

The clause also requires Contractors to timely disclose, in writing, to the agency Office of the Inspector General (OIG), with a copy to the Contracting Officer, whenever, in
connection with the award, performance, or closeout of this contract or any subcontract
thereunder, the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed—

1. A violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 of the United States Code; or
2. A violation of the civil False Claims Act (31 U.S.C. 3729-3733).

8.3.1 The contractor shall submit a final Trip Technical report including the SOVT documents against any effort related travel. The report shall address lessons learned and problem resolution for all issues encountered. **(CDRL A003/A004)**

8.4 COUNTERFEIT OR GREY MARKET INFORMATION TECHNOLOGY PRODUCTS

The statement below applies to all CLIN(s)

The contractor certifies that the product(s) being delivered are new and in their original packaging. The subject product(s) are eligible for all manufacturer warranties and other ancillary services or options provided by the original manufacturers, authorized suppliers, or suppliers that obtain parts from the manufacturer or its authorized supplier.

The contractor further certifies that it is authorized by the manufacturer to sell the product(s) and that it has provided documentation identifying its supply chain for the product(s) as required in the solicitation provisions. The contractor certifies that it accurately identified the country of manufacture in its proposal/quote and that the information provided remains the same.

The contractor assumes responsibility for authenticity. Costs of counterfeit parts are unallowable unless the conditions set forth in DFARS 231.205-71(b) are met.

By entering into this contract, the contractor acknowledges that a full or partial termination for default/cause for non-compliant awarded items may occur if any of the products provided are not recognized or acknowledged by the manufacturer as new products eligible for warranties and all other ancillary services or options provided by the manufacturer, or the offeror was not authorized by the manufacturer to sell the product in the U.S.

## 9.0 FACILITIES/INFRASTRUCTURE SUPPORT:

### 9.1 GENERAL HOUSEKEEPING:

The contractor shall implement their own policies and procedures in accordance with local requirements to provide for maintaining daily cleanliness of workspaces utilized by contractor personnel within a Government facility. The contractor shall perform monthly inspections to ensure cleanliness of workspaces. Any non-conformances shall be resolved within 2 weeks of identification.

### 9.2 SAFETY:

The contractor shall be cognizant and follow all safety regulations as those set forth by OSHA and any Government facility specific requirements, and is subject to unannounced Government inspections. This includes the use of personal protective equipment (PPE) as required in designated areas.

### 9.3 SOFTWARE:

The contractor shall provide sufficient software seats or licenses for drawing tools to effectively execute development of various technical data packages, installation drawings, and system engineering drawings required under this contract.

9.4 **HAND TOOLS:**

The contractor modernization/integration and engineering personnel shall provide their own basic hand tools.

**10.0 PLACE OF PERFORMANCE:**

The contractor will be required to work at NIWC (NIWC) Pacific, and the contractor's facilities. Work will also be performed at Navy and Joint DoD shore network installation sites worldwide. Specific places of performance will be identified at the task order level. The Government anticipates 95% of the work to be performed on site at a Government location (to include PWS 8.5) and 5% of the work to be performed at the contractor's site.

**11.0 PERIOD OF PERFORMANCE:**

The period of performance is anticipated to be a base period of one year, with four one-year option periods to be executed at the Government's discretion. Each optional Contract Line Item Number (CLIN) will have a separate and distinct period of performance not to exceed twelve (12) months, and must be exercised (if needed) within the contract period of performance.

**12.0 PERFORMANCE REQUIREMENTS:**

The Government will monitor and assess the contractor's performance against the Non-Performance Based Service Acquisition (non-PBSA) Surveillance Plan, which will assess Quality of Product or Services, Schedule, Cost Control, Management, Utlization of Small Business, and Regulatory Compliance and will be formally submitted via CPARs.

# NIWC Pacific SOW Addendum

## I. NIWC PACIFIC WORK WEEK

(a) All or a portion of the effort under this contract will be performed on a Government installation. The normal work week for Government employees at NIWC Pacific is Monday through Thursday 7:15 AM to 4:45 PM and Friday 7:15 AM to 3:45 PM with every other Friday a non-work day. Work at this Government installation, shall be performed by the contractor within the normal work hours at NIWC Pacific unless differing hours are specified on an individual delivery/task order. The contractor is not required to maintain the same hours as Government employees; however, contractor employees performing work at NIWC Pacific must work during the normal workweek. The following is a list of holidays observed by the Government.

| Name of Holiday | Time of Observance |
|---|---|
| New Year's Day | 1 January |
| Martin Luther King Jr. Day | Third Monday in January |
| Presidents Day | Third Monday in February |
| Memorial Day | Last Monday in May |
| Juneteenth National Independence Day | 19 June |
| Independence Day | 4 July |
| Labor Day | First Monday in September |
| Columbus Day | Second Monday in October |
| Veteran's Day | 11 November |
| Thanksgiving Day | Fourth Thursday in November |
| Christmas Day | 25 December |

(b) If any of the above holidays occur on a Saturday or a Sunday, then such holiday shall be observed by the contractor in accordance with the practice as observed by the assigned Government employees at the using activity.

(c) If the contractor is prevented from performance as the result of an Executive Order or an administrative leave determination applying to the using activity, such time may be charged to the contract as direct cost provided such charges are consistent with the contractor's accounting practices.

(d) This contract does not allow for payment of overtime during the normal workweek for employees who are not exempted from the Fair Labor Standards Act unless expressly authorized by the Ordering Officer. Under Federal regulations, the payment of overtime is required only when an employee works more than 40 hours during a week. Therefore, during the NIWC Pacific off-Friday (36-hour) week overtime will not be paid for non-exempt employees. During the work-Friday week (44 hour) the contractor is to schedule work so as not to incur overtime charges during the normal work week unless authorized in writing by the Government to do so. An example of this would be for contractor personnel to work during the hours of 7:15 AM to 4:45 PM Monday through Thursday and 7:15 AM to 3:45 PM Friday during the work-Friday week. The contractor may also

elect to configure the workforce in such a way that no single employee exceeds 40 hours during a normal week even though normal NIWC Pacific hours are maintained both weeks.

(2) (e) NOTICE: All contractor employees who make repeated deliveries to military installations shall obtain the required employee pass via the Defense Biometric Identification System (DBIDS) in order to gain access to the facility. Information about DBIDS may be found at the following website: https://www.cnic.navy.mil/om/dbids.html.
(3)
(4) Contractor employees must be able to obtain a DBIDS in accordance with base security requirements. Each employee shall wear the Government issued DBIDS badge over the front of the outer clothing. When an employee leaves the contractor's employ, the employee's DBIDS badge shall be returned to the Contracting Officer's Representative or the base Badge and Pass Office within five (5) calendar days.
(5)
(6) Contractors who do not have a DBIDS or Common Access Card (CAC) must be issued a one-day pass daily at the Badge and Pass Office. Issuance of a CAC requires the need for physical access to the installation and logical access to government owned computer systems.
(7)
(8) (f) Periodically, the Government may conduct Anti-Terrorism Force Protection (AT/FP) and/or safety security exercises, which may require the contractor to adjust its work schedule and/or place of performance to accommodate execution of the exercise. The contractor will be required to work with its Government point of contact to adjust work schedules and/or place of performance in the case of an exercise that causes disruption of normally scheduled work hours or disruption of access to a government facility. The contract does not allow for payment of work if schedules cannot be adjusted and/or the work cannot be executed remotely (i.e., the contractor's facility or alternate non-impacted location), during an exercise when government facilities are inaccessible.

## II. LIABILITY INSURANCE--COST TYPE CONTRACTS

(a) The following types of insurance are required in accordance with FAR 52.228-7 “Insurance--Liability to Third Persons” and shall be maintained in the minimum amounts shown:

(1) Workers’ compensation and employers’ liability: minimum of $100,000
(2) Comprehensive general liability: $500,000 per occurrence
(3) Automobile liability: $200,000 per person
$500,000 per occurrence
$ 20,000 per occurrence for property damage

(b) When requested by the contracting officer, the contractor shall furnish to the Contracting Officer a certificate or written statement of insurance. The written statement of insurance must contain the following information: policy number, policyholder, carrier, amount of coverage, dates of effectiveness (i.e., performance period), and contract number. The contract number shall be cited on the certificate of insurance.

## III. CONTRACTOR IDENTIFICATION

(a) Contractor employees must be clearly identifiable while on Government property by wearing appropriate badges.

(b) Contractor personnel and their subcontractors must identify themselves as contractors or subcontractors during meetings, telephone conversations, in electronic messages, or correspondence related to this contract.

(c) Contractor-occupied facilities (on Department of the Navy or other Government installations) such as offices, separate rooms, or cubicles must be clearly identified with contractor supplied signs, name plates or other identification, showing that these are work areas for contractor or subcontractor personnel.

## IV. REIMBURSEMENT OF TRAVEL COSTS

(a) Contractor Request and Government Approval of Travel

Any travel under this contract must be specifically requested in writing, by the contractor prior to incurring any travel costs. If this contract is an indefinite-delivery contract, then the written Government authorization will be by task/delivery orders issued by the Ordering Officer or by a modification to an issued task/delivery order. If this contract i an indefinite-delivery contract, then the written Government authorization will be by written notice of approval from the Contracting Officer's Representative (COR). The request shall, at a minimum, include:

(1) Contract number
(2) Date, time, and place of proposed travel
(3) Purpose of travel and how it relates to the contract
(4) Contractor's estimated cost of travel
(5) Name(s) of individual(s) traveling and;
(6) A breakdown of estimated travel and per diem charges.

(b) General

(1) The costs for travel, subsistence, and lodging shall be reimbursed to the contractor only to the extent that it is necessary and authorized for performance of the work under this contract. The costs for travel, subsistence, and lodging shall be reimbursed to the contractor in accordance with the Federal Acquisition Regulation (FAR) 31.205-46, which is incorporated by reference into this contract. As specified in FAR 31.205-46(a) (2), reimbursement for the costs incurred for lodging, meals and incidental expenses (as defined in the travel regulations cited subparagraphs (b)(1)(i) through (b)(1)(iii) below) shall be considered to be reasonable and

allowable only to the extent that they do not exceed on a daily basis the maximum per diem rates in effect at the time of travel as set forth in the following:

(i) Federal Travel Regulation prescribed by the General Services Administration for travel in the contiguous 48 United States;

(ii) Joint Travel Regulation, Volume 2, DoD Civilian Personnel, Appendix A, prescribed by the Department of Defense for travel in Alaska, Hawaii, The Commonwealth of Puerto Rico, and the territories and possessions of the United States; or

(iii) Standardized Regulations, (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances in Foreign Areas" prescribed by the Department of State, for travel in areas not covered in the travel regulations cited in subparagraphs (b)(1)(i) and (b)(1)(ii) above.

(2) Personnel in travel status from and to the contractor's place of business and designated work site or vice versa, shall be considered to be performing work under the contract, and contractor shall bill such travel time at the straight (regular) time rate; however, such billing shall not exceed eight hours per person for any one person while in travel status during one calendar day.

(c) Per Diem

(1) The contractor shall not be paid per diem for contractor personnel who reside in the metropolitan area in which the tasks are being performed. Per diem shall not be paid on services performed at contractor's home facility and at any facility required by the contract, or at any location within a radius of 50 miles from the contractor's home facility and any facility required by this contract.

(2) Costs for subsistence and lodging shall be paid to the contractor only to the extent that overnight stay is necessary and authorized in writing by the Government for performance of the work under this contract per paragraph (a). When authorized, per diem shall be paid by the contractor to its employees at a rate not to exceed the rate specified in the travel regulations cited in FAR 31.205-46(a)(2) and authorized in writing by the Government. The authorized per diem rate shall be the same as the prevailing locality per diem rate.

(3) Reimbursement to the contractor for per diem shall be limited to payments to employees not to exceed the authorized per diem and as authorized in writing by the Government per paragraph (a). Fractional parts of a day shall be payable on a prorated basis for purposes of billing for per diem charges attributed to subsistence on days of travel. The departure day from the Permanent Duty Station (PDS) and return day to the PDS shall be 75% of the applicable per diem rate. The contractor shall retain supporting documentation for per diem paid to employees as evidence of actual payments.

(d) Transportation

(1) The contractor shall be paid on the basis of actual amounts paid to the extent that such transportation is necessary for the performance of work under the contract and is authorized in writing by the Government per paragraph (a).

(2) The contractor agrees, in the performance of necessary travel, to use the lowest cost mode commensurate with the requirements of the mission and in accordance with good traffic management principles. When it is necessary to use air or rail travel, the contractor agrees to use coach, tourist class or similar accommodations to the extent consistent with the successful and economical accomplishment of the mission for which the travel is being performed. Documentation must be provided to substantiate non-availability of coach or tourist if business or first class is proposed to accomplish travel requirements.

(3) When transportation by privately owned conveyance (POC) is authorized, the contractor shall be paid on a mileage basis not to exceed the applicable Government transportation rate specified in the travel regulations cited in FAR 31.205-46(a)(2) and is authorized in writing by the Government per paragraph (a).

(4) When transportation by privately owned (motor) vehicle (POV) is authorized, required travel of contractor personnel, that is not commuting travel, may be paid to the extent that it exceeds the normal commuting mileage of such employee. When an employee's POV is used for travel between an employee's residence or the Permanent Duty Station and one or more alternate work sites within the local area, the employee shall be paid mileage for the distance that exceeds the employee's commuting distance.

(5) When transportation by a rental automobile, other special conveyance or public conveyance is authorized, the contractor shall be paid the rental and/or hiring charge and operating expenses incurred on official business (if not included in the rental or hiring charge). When the operating expenses are included in the rental or hiring charge, there should be a record of those expenses available to submit with the receipt. Examples of such operating expenses include hiring charge (bus, streetcar or subway fares), gasoline and oil, parking, and tunnel tolls.

(6) Definitions:

(i) "Permanent Duty Station" (PDS) is the location of the employee's permanent work assignment (i.e., the building or other place where the employee regularly reports for work.

(ii) "Privately Owned Conveyance" (POC) is any transportation mode used for the movement of persons from place to place, other than a Government conveyance or common carrier, including a conveyance loaned for a charge to, or rented at personal expense by, an employee for transportation while on travel when such rental conveyance has not been authorized/approved as a Special Conveyance.

(iii) "Privately Owned (Motor) Vehicle (POV)" is any motor vehicle (including an automobile, light truck, van or pickup truck) owned by, or on a long-term lease (12 or more months) to, an employee or that employee's dependent for the primary purpose of providing personal transportation, that:

(a) is self-propelled and licensed to travel on the public highways;
(b) is designed to carry passengers or goods; and
(c) has four or more wheels or is a motorcycle or moped.

(iv) "Special Conveyance" is commercially rented or hired vehicles other than a POC and other than those owned or under contract to an agency.

(v) "Public Conveyance" is local public transportation (e.g., bus, streetcar, subway, etc.) or taxicab.

(iv) "Residence" is the fixed or permanent domicile of a person that can be reasonably justified as a bona fide residence.

EXAMPLE 1: Employee's one way commuting distance to regular place of work is 7 miles. Employee drives from residence to an alternate work site, a distance of 18 miles. Upon completion of work, employee returns to residence, a distance of 18 miles.

*In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal round trip commuting distance (14 miles). The employee is reimbursed for 22 miles (18 + 18 - 14 = 22).*

EXAMPLE 2: Employee's one way commuting distance to regular place of work is 15 miles. Employee drives from residence to an alternate work site, a distance of 5 miles. Upon completion of work, employee returns to residence, a distance of 5 miles.

*In this case, the employee is not entitled to be reimbursed for the travel performed (10 miles), since the distance traveled is less than the commuting distance (30 miles) to the regular place of work.*

EXAMPLE 3: Employee's one way commuting distance to regular place of work is 15 miles. Employee drives to regular place of work. Employee is required to travel to an alternate work site, a distance of 30 miles. Upon completion of work, employee returns to residence, a distance of 15 miles.

*In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal round trip commuting distance (30 miles). The employee is reimbursed for 30 miles (15 + 30 + 15 - 30 = 30).*

EXAMPLE 4: Employee's one way commuting distance to regular place of work is 12 miles. In the morning, the employee drives to an alternate work site (45 miles). In the afternoon, the

employee returns to the regular place of work (67 miles). After completion of work, employee returns to residence, a distance of 12 miles.

*In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal round trip commuting distance (24 miles). The employee is reimbursed for 100 miles (45 + 67 + 12 - 24 = 100).*

EXAMPLE 5: Employee's one way commuting distance to regular place of work is 35 miles. Employee drives to the regular place of work (35 miles). Later, the employee drives to alternate work site #1 (50 miles) and then to alternate work site #2 (25 miles). Employee then drives to residence (10 miles).

*In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal commuting distance (70 miles). The employee is reimbursed for 50 miles (35 + 50 + 25 + 10 - 70 = 50).*

EXAMPLE 6: Employee's one way commuting distance to regular place of work is 20 miles. Employee drives to the regular place of work (20 miles). Later, the employee drives to alternate work site #1 (10 miles) and then to alternate work site #2 (5 miles). Employee then drives to residence (2 miles).

*In this case, the employee is not entitled to be reimbursed for the travel performed (37 miles), since the distance traveled is less than the commuting distance (40 miles) to the regular place of work.*

## V. REQUIRED INFORMATION ASSURANCE AND PERSONNEL SECURITY REQUIREMENTS FOR ACCESSING GOVERNMENT INFORMATION SYSTEMS AND NONPUBLIC INFORMATION

(a) Definition. As used in this text, "sensitive information" includes:

(i) All types and forms of confidential business information, including financial information relating to a contractor's pricing, rates, or costs, and program information relating to current or estimated budgets or schedules;
(ii) Source selection information, including bid and proposal information as defined in FAR 2.101 and FAR 3.104-4, and other information prohibited from disclosure by the Procurement Integrity Act (41 USC 423);
(iii) Information properly marked as "business confidential," "proprietary," "procurement sensitive," "source selection sensitive," or other similar markings;
(iv) Other information designated as sensitive by the Naval Information Warfare Systems Command (NAVWAR).

(b) In the performance of the contract, the contractor may receive or have access to information, including information in Government information systems and secure websites. Accessed information may include "sensitive information" or other information not previously made available to the public that would be competitively useful on current or future related procurements.

(c) Contractors are obligated to protect and safeguard from unauthorized disclosure all sensitive information to which they receive access in the performance of the contract, whether the information comes from the Government or from third parties. The contractor shall—

(i) Utilize accessed information and limit access to authorized users only for the purposes of performing the services as required by the contract, and not for any other purpose unless authorized;
(ii) Safeguard accessed information from unauthorized use and disclosure, and not discuss, divulge, or disclose any accessed information to any person or entity except those persons authorized to receive the information as required by the contract or as authorized by Federal statute, law, or regulation;
(iii) Inform authorized users requiring access in the performance of the contract regarding their obligation to utilize information only for the purposes specified in the contact and to safeguard information from unauthorized use and disclosure.
(iv) Execute a "Contractor Access to Information Non-Disclosure Agreement," and obtain and submit to the Contracting Officer a signed "Contractor Employee Access to Information Non-Disclosure Agreement" for each employee prior to assignment;
(v) Notify the Contracting Officer in writing of any violation of the requirements in (i) through (iv) above as soon as the violation is identified, no later than 24 hours. The notice shall include a description of the violation and the proposed actions to be taken, and shall include the business organization, other entity, or individual to whom the information was divulged.

(d) In the event that the contractor inadvertently accesses or receives any information marked as "proprietary," "procurement sensitive," or "source selection sensitive," or that, even if not properly marked otherwise indicates the contractor may not be authorized to access such information, the contractor shall (i) notify the Contracting Officer; and (ii) refrain from any further access until authorized in writing by the Contracting Officer.

(e) The requirements of this text are in addition to any existing or subsequent Organizational Conflicts of Interest (OCI) requirements which may also be included in the contract, and are in addition to any personnel security or Information Assurance requirements, including Systems Authorization Access Request (SAAR-N), DD Form 2875, Annual Information Assurance (IA)

training certificate, SF85P, or other forms that may be required for access to Government information systems.

(f) Subcontracts. The contractor shall insert paragraphs (a) through (f) of this text in all subcontracts that may require access to sensitive information in the performance of the contract.

(g) Mitigation Plan. If requested by the Contracting Officer, the contractor shall submit, within 45 calendar days following execution of the "Contractor Non-Disclosure Agreement," a mitigation plan for Government approval, which shall be incorporated into the contract. At a minimum, the mitigation plan shall identify the contractor's plan to implement the requirements of paragraph (c) above and shall include the use of a firewall to separate contractor personnel requiring access to information in the performance of the contract from other contractor personnel to ensure that the contractor does not obtain any unfair competitive advantage with respect to any future Government requirements due to unequal access to information. A "firewall" may consist of organizational and physical separation; facility and workspace access restrictions; information system access restrictions; and other data security measures identified, as appropriate. The contractor shall respond promptly to all inquiries regarding the mitigation plan. Failure to resolve any outstanding issues or obtain approval of the mitigation plan within 45 calendar days of its submission may result, at a minimum, in rejection of the plan and removal of any system access.

## VI. DESIGNATION OF CONTRACTING OFFICER'S REPRESENTATIVE

The Contracting Officer hereby appoints the following individual as Contracting Officer's Representative (COR) for this contract/order:

Name: Jamie Saenz
Code: 55380
Phone Number: (619) 887-5061
E-mail: jaime.e.saenz.civ@us.navy.mil

## VII. TECHNICAL DIRECTION

(a) Technical Direction may be provided to the contractor from time to time by the Contracting Officer or Contracting Officer's Representative, if authorized, during the term (term is defined as the period of performance for the basic contract and any options that may be exercised) of this contract. Technical Direction will provide specific information relating to the tasks contained in the Statement of Work and will be provided to the contractor in writing. Any Technical Direction issued hereunder will be subject to the terms and conditions of the contract. The contract shall

take precedence if there is any conflict with any Technical Direction issued hereunder, and cannot be modified by any Technical Direction.

(b) As stated, Technical Direction shall be issued in writing and shall include, but not be limited to:

(1) date of issuance of Technical Direction;
(2) applicable contract number;
(3) technical direction identification number;
(4) description of Technical Direction;
(5) estimated cost;
(6) estimated level of effort by labor category; and
(7) signature of the PCO or COR.

(c) If the contractor does not agree with the estimated cost specified on the technical direction, or considers the technical direction to be outside the scope of the contract, it shall notify the PCO or COR immediately and, in the case of the estimated cost, arrive at a general agreement to the cost of the task. In the case of the direction requiring work that is out of the scope of the contract, the contractor shall not proceed with the effort unless and until the PCO executes a contract modification to include the change in scope.

## VIII. POST-AWARD IDENTIFICATION AND ASSERTION OF RESTRICTIONS ON TECHNICAL DATA PERTAINING TO A COMMERCIAL ITEM AND COMMERCIAL COMPUTER SOFTWARE

a. Definitions. Unless otherwise specified in this provision, the terms used in this provision are defined in the FAR/DFARS, as applicable.

b. Post-award Assertions. In addition to the pre-award assertions made, other assertions on technical data pertaining to a commercial item and commercial computer software may be identified after award when based on new information or inadvertent omissions, unless the inadvertent omissions would have materially affected the source selection decision. Such identifications and assertions shall be submitted to the contracting officer as soon as practicable prior to the scheduled date for delivery of the technical data/computer software, using the table format found below and signed by an official authorized to contractually obligate the contractor.

| Commercial Technical Data/Computer Software Title, Version #, and License* | Technical Use/ Implementing Approach ** | If OSS, Was OSS modified by Contractor? *** | Name of Contractor Delivering Commercial Software**** |
|---|---|---|---|
| | | | |

* For commercial technical data (other than computer software documentation) pertaining to items, components, or processes developed at private expense, identify both the deliverable technical data and each such item, component, or process. For computer software or computer software documentation identify the computer software or computer software documentation. The complete title and version number of the computer software should be listed. If Open Source Software (OSS), the OSS license and version number should be listed. If a version number is not available, the contractor should state no version number. If commercial technical data is being delivered under the terms of DFARS 252.227-7015, then DFARS 252.227-7015 should be listed. If the OSS was downloaded from a website, the website address should also be provided. Enter none if all commercial technical data or commercial computer software will be submitted without restrictions.

** The functionality of the commercial computer software should be described, as well as where it is being used within the larger computer software deliverable (if applicable).

*** If OSS is being used, the contractor should state whether it has modified the OSS.

**** Corporation, individual, or other person as appropriate.

c. Licenses. The contractor shall provide copies of all commercial license(s) for the commercial technical data or commercial computer software that will be delivered. The Government will review the licenses to ensure that the license terms are consistent with federal procurement law and meet the Government's end user needs.

d. Use of OSS Without Delivery. The Government treats OSS as a category of commercial computer software. If the contractor proposes to use, but not deliver, commercial computer software (including OSS), the contractor must ensure that such use does not: (i) create, or purport to create, any Government distribution obligations with respect to the computer software deliverables; or (ii) grant, or purport to grant, to any third party any rights to or immunities under Government intellectual property or Government data rights to the Government computer software deliverables.

## IX. OFFSHORE PROCUREMENT OF COMSEC EQUIPMENT

Due to the sensitivity of Communications Security (COMSEC) and to maintain rigid control over the integrity of COMSEC equipment, no subcontracts or purchase orders which involve design, manufacture, production, assembly or test in a location not in the United States, of equipment, assemblies, accessories or parts performing cryptographic functions shall be made under this contract without prior specific approval of the Contracting Officer. The contractor further agrees to include this text in all subcontracts it may issue pursuant to this contract for equipment, assemblies, accessories or parts.

## X. CYBERSECURITY

Cybersecurity (which replaced the term Information Assurance (IA)) is defined as prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Contractor personnel shall perform tasks to ensure Navy applications, systems, and networks satisfy Federal/DoD/DON/Navy cybersecurity requirements.

**Cyber IT and Cybersecurity Personnel**

(a) The Cyberspace workforce elements addressed include contractors performing functions in designated Cyber IT positions and Cybersecurity positions. In accordance with DFARS Subpart 239.71, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, contractor personnel performing cybersecurity functions shall meet all cybersecurity training, certification, and tracking requirements as cited in DoD 8570.01-M prior to accessing DoD information systems. Proposed contractor Cyber IT and cybersecurity personnel shall be appropriately qualified prior to the start of the contract performance period or before assignment to the contract during the course of the performance period.

(b) The contractor shall be responsible for identifying, tracking and reporting cybersecurity personnel, also known as Cybersecurity Workforce (CSWF) and Cyber IT workforce personnel. Although the minimum frequency of reporting is monthly, the task order can require additional updates at any time.

(c) Contractors that access Navy IT shall also follow guidelines and provisions documented in Navy Telecommunications Directive (NTD 10-11) and are required to complete a System Authorization Access Request (SAAR) – Navy form as documented in para 8.2.2.4(b).

When a contractor requires logical access to a government IT system or resource (directly or indirectly), the required CAC will have a Public Key Infrastructure (PKI). A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-M-V1, CAC PKI certificates will be associated with an official government issued e-mail address (e.g., .mil, .gov, .edu). Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the contract's specified COR. Note: In order for personnel to maintain a CAC with PKI, each contractor employee shall complete annual cybersecurity training. The following guidance for training and form submittal is provided; however, contractors shall seek latest guidance from their appointed company Security Officer and the NIWC Pacific Information Assurance Management (IAM) office:

1. For annual DoD Cybersecurity/IA Awareness training, contractors shall use this site: https://twms.nmci.navy.mil/. For those contractors requiring initial training and do not have a CAC, contact the NIWC Pacific IAM office. Training can be taken at the IAM office or online at http://iase.disa.mil/index2.html.

2. For SAAR-N form, the contractor shall use OPNAV 5239/14 (Rev 9/2011). Contractors can obtain a form from the NIWC Pacific IAM office or from the website: https://navalforms.documentservices.dla.mil/.

(d) Contractor personnel with privileged access will be required to acknowledge special responsibilities with a Privileged Access Agreement (PAA) IAW SECNAVINST 5239.20A.

**Design, Integration, Configuration or Installation of Hardware and Software**

The contractor shall ensure any equipment/system installed or integrated into Navy platform will meet the cybersecurity requirements as specified under DoDI 8500.01. The contractor shall ensure that any design change, integration change, configuration change, or installation of hardware and software is in accordance with established DoD/DON/Navy cyber directives and does not violate the terms and conditions of the accreditation/authorization issued by the appropriate Accreditation/Authorization official. Contractors that access Navy IT are also required to follow the provisions contained in DON CIO Memorandum:

Acceptable Use of Department of the Navy Information Technology (IT) dated 12 Feb 16. Use of blacklisted software is specifically prohibited and only software that is registered in DON Application and Database Management System (DADMS) and is Functional Area Manager (FAM) approved can be used as documented in para 5.2.2. Procurement and installation of software governed by DON Enterprise License Agreements (ELAs) – Microsoft, Oracle, Cisco, Axway, Symantec, ActivIdentity, VMware, Red Hat, NetApp, and EMC shall be in accordance with DON CIO Policy and DON ELAs awarded.

**Cybersecurity Workforce (CSWF) Report**

DoD 8570.01-M and DFARS PGI 239.7102-3 have promulgated that contractor personnel shall have documented current cybersecurity certification status within their contract. The contractor shall develop, maintain, and submit a CSWF Report as applicable at the task order level. IAW DFARS clause 252.239-7001, if cybersecurity support is provided, the contractor shall provide a Cybersecurity Workforce (CSWF) list that identifies those individuals who are IA trained and certified. Utilizing the format provided at the task order level, the prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. See applicable DD Form 1423 for additional reporting details and distribution instructions. Contractor shall verify with the COR or other government representative the proper labor category cybersecurity designation and certification requirements.

**Information Technology (IT) Services Requirements**

This paragraph only applies to IT contracts. Information Technology (IT) is defined as any equipment or interconnected system(s) or subsystem(s) of equipment that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data of information by the agency. IT includes computers, ancillary equipment, peripherals, input, output, and storage

devices necessary for security and surveillance. Electronic and Information technology (EIT) is IT that is used in the creation, conversion, or duplication of data or information. EIT includes: telecommunication products, such as telephones; information kiosks; transaction machines; World Wide Web sites; multimedia (including videotapes); and office equipment, such as copiers and fax machines.

**Information Technology (IT) General Requirements**

When applicable, the contractor shall be responsible for the following:

• Ensure that no production systems are operational on any RDT&E network.
• Follow DoDI 8510.01 of 12 Mar 2014 when deploying, integrating, and implementing IT capabilities.
• Migrate all Navy Ashore production systems to the NMCI environment where available.
• Work with government personnel to ensure compliance with all current Navy IT & cybersecurity policies, including those pertaining to Cyber Asset Reduction and Security (CARS).
• Follow SECNAVINST 5239.3B of 17 June 2009 & DoDI 8510.01 of 12 Mar 2014 prior to integration and implementation of IT solutions or systems.
• Register any contractor-owned or contractor-maintained IT systems utilized on contract in the Department of Defense IT Portfolio Registry (DITPR)-DON.
• Only perform work specified within the limitations of the task order.

**Acquisition of Commercial Software Products, hardware, and Related Services**

This paragraph only applies to the purchasing/hosting of commercial software. Contractors recommending or purchasing commercial software products, hardware, and related services supporting Navy programs and projects shall ensure they recommend or procure items from approved sources in accordance with the latest DoN and DoD policies.

**DON Enterprise Licensing Agreement/DOD Enterprise Software Initiative Program**

Pursuant to DoN Memorandum – Mandatory use of DoN Enterprise Licensing Agreement (ELA) dated 22 Feb 12, contractors that are authorized to use Government supply sources per FAR 51.101 shall verify if the product is attainable through DoN ELAs and if so, procure that item in accordance with appropriate ELA procedures. If an item is not attainable through the DoN ELA program, contractors shall then utilize DoD Enterprise Software Initiative (ESI) program (see DFARS 208.74) and government-wide SmartBuy program (see DoD memo dated 22 Dec 05). The contractor shall ensure any items purchased outside these programs have the required approved waivers as applicable to the program. Software requirements will be specified at the task order level.

**DON Application and Database Management System**

The contractor shall ensure that no Functional Area Manager (FAM) disapproved applications are integrated, installed or operational on Navy networks. The contractor shall ensure that all databases that use database management systems (DBMS) designed, implemented, and/or hosted on servers and/or mainframes supporting Navy applications and systems be registered in DoN Application and Database Management System (DADMS) and are FAM approved. All integrated, installed, or operational applications hosted on Navy networks must also be registered in DADMS and approved by the FAM. No operational systems or applications will be integrated, installed, or operational on the RDT&E network.

**Section 508 Compliance**

This paragraph only applies to IT contracts. The contractor shall ensure that all software recommended, procured, and/or developed is compliant with Section 508 of the Rehabilitation Act of 1973, 26 CFR Part 1194 and pursuant to SPAWARINST 5721.1B of 17 Nov 2009. In accordance with FAR 39.204, this requirement does not apply to contractor acquired software that is incidental to the task, software procured/developed to support a program or system designated as a National Security System (NSS) or if the product is located in spaces frequented only by service personnel for maintenance, repair or occasional monitoring of equipment.

**Software Development/Modernization and Hosting**

This paragraph only applies to software development and modernization. The contractor shall ensure all programs utilizing this contract for software development/ modernization (DEV/MOD), including the development of IT tools to automate NIWC Pacific business processes are compliant with DON Information Management/Information Technology (DON IM/IT) Investment Review Process Guidance requirements. Contractors shall neither host nor develop IT tools to automate NIWC Pacific business processes unless specifically tasked within the task order or contract. The contractor shall ensure IT tools developed to automate NIWC Pacific business processes will be delivered with full documentation and source code, as specified at the task order level, to allow non-proprietary operation and maintenance by any source. The contractor shall ensure all programs are submitted with proof of completed DEV/MOD certification approval from the appropriate authority in accordance with DON policy prior to task order award. *Note must be listed on Investment Review Board (IRB) approved list.

**Information Security**

Pursuant to DoDM 5200.01 and DoD 5200.48, the contractor shall provide adequate security for all CUI and unclassified DoD information passing through non-DoD information systems, including all subcontractor information systems utilized on contract. If the contractor originates, adds, or changes any of the DoD information, it must be marked in accordance with DODI 5200.48 and handled properly. The contractor shall disseminate CUI and unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking).

**IT Position Designations**

Pursuant to DoDI 8500.01, DoD 8570.01-M, SECNAVINST 5510.30, SECNAV M-5239.2, and applicable to unclassified DoD information systems, a designator is assigned to certain individuals that indicates the level of Special-Sensitive (SS)/Critical-Sensitive (CS) or Noncritical Sensitive (NCS), access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. Per SECNAVINST 5510.30C, page 7, Section 8.b of enclosure (4), the Information Systems Security Manager is responsible for establishing, implementing and maintaining the DoN information system and information assurance program and is responsible to the Commanding Officer for developing, maintaining, and directing the implementation of the Information Assurance (IA) program within the command. The three basic position sensitivity levels/Position Designations:

Special-Sensitive (SS)/T5 or T5R; equivalent (SSBI, etc.) (IT Level I) - Potential for inestimable impact and/or damage.

Critical-Sensitive (CS)/T5 or T5R; equivalent (SSBI, etc.) (IT Level I) - Potential for grave to exceptionally grave impact and/or damage.

Noncritical Sensitive (NCS)/T3 or T3R; equivalent (ANAC/ANACI) (IT Level II) - Potential for some to serious impact and/or damage.

## XI. SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

**1. <u>System Security Plan and Plans of Action and Milestones (SSP/POAM) Reviews</u>**

a) Within thirty (30) days of contract award, the Contractor shall make its System Security Plan(s) (SSP(s)) for its covered contractor information system(s) available for review by the Government at the contractor's facility. The SSP(s) shall implement the security requirements in Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, which is included in this contract. The Contractor shall fully cooperate in the Government's review of the SSPs at the Contractor's facility.

b) If the Government determines that the SSP(s) does not adequately implement the requirements of DFARS clause 252.204-7012 then the Government shall notify the Contractor of each identified deficiency. The Contractor shall correct any identified deficiencies within thirty (30) days of notification by the Government. The contracting officer may provide for a correction period longer than thirty (30) days and, in such a case, may require the Contractor to submit a plan of action and milestones (POAM) for the correction of the identified deficiencies. The Contractor shall immediately notify the contracting officer of any failure or anticipated failure to meet a milestone in such a POAM.

c) Upon the conclusion of the correction period, the Government may conduct a follow-on review of the SSP(s) at the Contractor's facilities. The Government may continue to conduct follow-on reviews until the Government determines that the Contractor has corrected all identified deficiencies in the SSP(s).
d) The Government may, in its sole discretion, conduct subsequent reviews at the Contractor's site to verify the information in the SSP(s). The Government will conduct such reviews at least every three (3) years (measured from the date of contract award) and may conduct such reviews at any time upon thirty (30) days' notice to the Contractor.

**2. <u>Compliance to NIST 800-171</u>**

a) The Contractor shall fully implement the CUI Security Requirements (Requirements) and associated Relevant Security Controls (Controls) in NIST Special Publication 800-171 (Rev. 1) (NIST SP 800-171), or establish a SSP(s) and POA&Ms that varies from NIST 800-171 only in accordance with DFARS clause 252.204-7012(b)(2), for all covered contractor information systems affecting this contract.
b) Notwithstanding the allowance for such variation, the contractor shall identify in any SSP and POA&M their plans to implement the following, at a minimum:
   (1) Implement Control 3.5.3 (Multi-factor authentication). This means that multi-factor authentication is required for all users, privileged and unprivileged accounts that log into a network. In other words, any system that is not standalone should be required to utilize acceptable multi-factor authentication. For legacy systems and systems that cannot support this requirement, such as CNC equipment, etc., a combination of physical and logical protections acceptable to the Government may be substituted;
   (2) Implement Control 3.1.5 (least privilege) and associated Controls, and identify practices that the contractor implements to restrict the unnecessary sharing with, or flow of, covered defense information to its subcontractors, suppliers, or vendors based on need-to-know principles;
   (3) Implement Control 3.1.12 (monitoring and control remote access sessions) - Require monitoring and controlling of remote access sessions and include mechanisms to audit the sessions and methods.
   (4) Audit user privileges on at least an annual basis;
   (5) Implement:
      i. Control 3.13.11 (FIPS 140-2 validated cryptology or implementation of NSA or NIST approved algorithms (i.e. FIPS 140-2 Annex A: AES or Triple DES) or compensating controls as documented in a SSP and POAM); and,
      ii. NIST Cryptographic Algorithm Validation Program (CAVP) (see https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program);
   (6) Implement Control 3.13.16 (Protect the confidentiality of CUI at rest) or provide a POAM for implementation which shall be evaluated by the Navy for risk acceptance.
   (7) Implement Control 3.1.19 (encrypt CUI on mobile devices) or provide a plan of action for implementation which can be evaluated by the Government Program Manager for risk to the program.

**3. Cyber Incident Response:**

a) The Contractor shall, within fifteen (15) days of discovering the cyber incident (inclusive of the 72-hour reporting period), deliver all data used in performance of the contract that the Contractor determines is impacted by the incident and begin assessment of potential warfighter/program impact.

b) Incident data shall be delivered in accordance with the Department of Defense Cyber Crimes Center (DC3) Instructions for Submitting Media available at http://www.acq.osd.mil/dpap/dars/pgi/docs/Instructions_for_Submitting_Media.docx. In delivery of the incident data, the Contractor shall, to the extent practical, remove contractor-owned information from Government covered defense information.

c) If the Contractor subsequently identifies any such data not previously delivered to DC3, then the Contractor shall immediately notify the contracting officer in writing and shall deliver the incident data within ten (10) days of identification. In such a case, the Contractor may request a delivery date later than ten (10) days after identification. The contracting officer will approve or disapprove the request after coordination with DC3.

**4. Naval Criminal Investigative Service (NCIS) Outreach**

The Contractor shall engage with NCIS industry outreach efforts and consider recommendations for hardening of covered contractor information systems affecting DON programs and technologies.

**5. NCIS/Industry Monitoring**

a) In the event of a cyber incident or at any time the Government has indication of a vulnerability or potential vulnerability, the Contractor shall cooperate with the Naval Criminal Investigative Service (NCIS), which may include cooperation related to: threat indicators; pre-determined incident information derived from the Contractor's infrastructure systems; and the continuous provision of all Contractor, subcontractor or vendor logs that show network activity, including any additional logs the contractor, subcontractor or vendor agrees to initiate as a result of the cyber incident or notice of actual or potential vulnerability.

b) If the Government determines that the collection of all logs does not adequately protect its interests, the Contractor and NCIS will work together to implement additional measures, which may include allowing the installation of an appropriate network device that is owned and maintained by NCIS, on the Contractor's information systems or information technology assets. The specific details (e.g., type of device, type of data gathered, monitoring period) regarding the installation of an NCIS network device shall be the subject of a separate agreement negotiated between NCIS and the Contractor. In the alternative, the Contractor may install network sensor capabilities or a network monitoring service, either of which must be reviewed for acceptability by NCIS. Use of this alternative approach shall also be the subject of a separate agreement negotiated between NCIS and the Contractor.

c) In all cases, the collection or provision of data and any activities associated with this statement of work shall be in accordance with federal, state, and non-US law.

## XII. INTELLIGENCE OVERSIGHT

In compliance with DoDD 5148.13 paragraph 4.1.e and SECNAVINST 3820.3F, for any contractor personnel conducting Intelligence or Intelligence-related activities or supporting those efforts under Department of Defense authorities shall report any Questionable Intelligence Activity (QIA), Significant, or Highly Sensitive Matter (S/HSM) to the Naval Information Warfare Systems Command Intelligence Oversight Program Manager or Senior Intelligence Officer.

**Questionable Intelligence Activity (QIA):** Any Intelligence or Intelligence-related activity when there is reason to believe such activity may be unlawful or contrary to an Executive Order, Presidential Directive, Intelligence Community Directive, or applicable DoD policy governing that activity.

**Significant or Highly Sensitive Matter (S/HSM):** An Intelligence or Intelligence-related activity (regardless of whether the Intelligence or Intelligence-related activity is unlawful or contrary to an Executive Order, Presidential Directive, Intelligence Community Directive, or DoD policy), or serious criminal activity by Intelligence personnel, that could impugn the reputation or integrity of the Intelligence Community, or otherwise call into question the propriety of Intelligence activities. Such matters might involve actual or potential:

- Congressional inquiries or investigations
- Adverse media coverage
- Impact on foreign relations or foreign partners
- Systemic compromise, loss, or unauthorized disclosure of protected information.

## XIII. CONTRACTOR FURNISHED EQUIPMENT ON RDT&E NETWORKS

Contractors are prohibited from connecting any non-Government owned equipment to RDT&E networks unless the equipment is specifically identified hereunder. The following contractor owned/provided equipment is permitted to be connected to the RDT&E network, as necessitated by the statement of work, in performance of this contract only:

- None

Any changes to this list must be completed via formal contract modification prior to implementation or use on the network. Before connection of any above-listed equipment is made, the Command Information System Security Manager (Code 82400) must be informed via Cybersecurity Exception Request. All other equipment not specifically identified above remains prohibited for use on RDT&E networks.

Per the DON Destruction of Electronic Storage Media Policy, all contractor-provided internal and removable electronic storage media listed above shall become Government property upon the sooner of: equipment end of life, replacement, end of service, or turn-in; contract completion, or contract termination. The contractor shall work with the Contracting Officer or Contracting Officer's Representative (COR), if applicable, to facilitate the immediate turnover of internal and removable electronic storage media as soon as one of the aforementioned circumstances arise.

Internal and removable electronic storage media includes, but is not limited to, workstations, laptops/notebooks, printers, copiers, scanners, multi-functional devices (MFD), and hand held devices with internal storage devices, removable hard drives, external hard drives, solid state hard drives, flash based storage media such as "thumb" drives and camera memory cards, backup data systems (e.g., DAT, LTO, DLT), and optical storage devices (e.g., CD/DVD).

## XIV. CONTRACTOR COMPLIANCE WITH FOREIGN ENTRY REQUIREMENTS

Contractor personnel performing contracts outside of the United States must comply with the entry requirements of the respective geographic combatant command (GCC) and all applicable host nation procedures. These entry/clearance requirements are stipulated on a country-by-country basis in the Electronic Foreign Clearance Guide (EFCG), located at https://www.fcg.pentagon.mil. Compliance with the EFCG is required for all contractor personnel traveling outside of the United States in support of this contract. Contractor personnel are responsible for ensuring they obtain access to the EFCG by requesting a username and password at https://www.fcg.pentagon.mil, and that all foreign entry requirements are met.

## XV. TRADEMARK RIGHTS (OLD PROGRAM)

The contractor shall not assert any claim, in any jurisdiction, based on trademark or other name or design-based causes of action that are based on rights the contractor believes it has in the term(s) such as names, words, acronyms, symbols, logos, seals, emblems used or intended to be used by the DoN acquisition programs addressed in this contract's statement of work or performance work statement (the "Designation(s)"), against the Government or others authorized by the Government to use the Designation(s) (including the word(s), name, symbol, or design) acting within the scope of such authorization (i.e. claims for trademark infringement, dilution, trade dress infringement, unfair competition, false advertising, palming off, passing off, or counterfeiting). Such authorization shall be implied by the award of a Government contract to any party for the manufacture, production, distribution, use, modification, maintenance, sustainment, or packaging of the products and services identified under this contract, and the scope of such implied authorization is defined as the use of the Designation(s) in performance under such contract by the prime contractor and its subcontractors and suppliers at any tier. In all other cases, the scope of the authorization will be defined by the Government in writing.

## XVI. PERSONNEL SECURITY PROGRAM REQUIREMENTS FOR UNCLASSIFIED/POSITION OF TRUST (POT) CONTRACTORS

The U.S. Government conducts Fitness Determination investigations of personnel who are assigned to positions that directly or indirectly affect the operation of unclassified IT resources and systems that process Department of Defense (DoD) information, to include For Official Use Only (FOUO) and other controlled unclassified information (CUI) in accordance with DODM 5220.22 Volume 2 (National Industrial Security Program: Industrial Security Procedures for Government Activities) and for additional guidance refer to DoDI 5200.48.

The United States Office of Personnel Management (OPM), and Defense Counterintelligence and Security Agency (DCSA) process all requests for U.S. Government Fitness Determination investigations. Requirements for these investigations are outlined in NAVWAR M5510.1A, Chapter 5005.4 and NIWCPACINST 5500.1C, Chapter 9.4.4.

**I. Procedures for submitting U.S. Government Fitness Determination Investigations:**

A Fitness Determination investigation supports a Public Trust position; it does NOT support a National Security Eligibility position.

Only the e-QIP version of the SF 86 are acceptable by OPM-DCSA.

After determining that an individual requires Public Trust Position determination, the FSO will identify the individual to the COR. The FSO will also provide the following information to the COR so that the NIWC PAC Personnel Security Office can initiate a request thru e-QIP:

Full SSN of the applicant, Full Name, Date of Birth, Place of Birth, Email Address and Phone Number

A contractor worksheet will be provided by Personnel Security for the COR and/or the FSO to complete that includes the above information and any additional information required by the Personnel Security Office.

The Personnel Security Office will send email notification and instructions to the applicant to complete and submit e-QIP expeditiously.

The FSO will take and submit fingerprints via electronic submission. If the FSO does not have the means to submit fingerprints electronically, they will obtain hardcopy fingerprints using SF-87 or FD-258. For immediate fingerprint result, electronic transmission of fingerprints is encouraged. OPM no longer accepts the submission of hard copy fingerprints (SF-87 or FD-258).

If fingerprints are obtained via hardcopy, the hardcopies will be sent to NIWC PAC Personnel Security via USPS Priority mail:

Commanding Officer, NIWC PAC
ATTN: Personnel Security, Code 83310
53560 Hull St
San Diego CA 92152

Contractor Fitness Determinations made by the DOD CAF are maintained in the Defense Information System for Security (DISS). Favorable Fitness Determinations will support Public Trust positions only and not National Security Eligibility positions. If no issues are discovered, according to respective guidelines, a HSPD-12 Determination will be populated in DISS and will be reciprocal within DoN. If issues are discovered, the DOD CAF will forward the investigation along with all supporting documentation to the NIWC PAC Security Office for local determination. The Command Security Manager will make the local Fitness Determination and your company will be notified of the decision in writing. If an individual receives a negative Fitness Determination, they will be immediately removed from their position of trust, the FSO will be notified, and the company will replace any individual who has received a negative Fitness Determination.

If you require additional assistance with the submission of Public Trust Investigations, you may send an email to NIWC PAC Personnel Security at NIWC_PAC_UNCLASSCTR@NAVY.MIL.

**II. Employment Terminations:**

The contractor shall:
- Immediately notify the COR or TR of the employee's termination.
- Send email to NIWC_PAC_UNCLASSCTR@NAVY.MIL, Code 83310 notifying them of the termination.
- Fax a termination VAL to Code 83320 at (619) 553-6169.
- Return any badge and decal to Commanding Officer, Naval Information Warfare Center Pacific, Attn: Code 83320, 53560 Hull Street, San Diego, CA 92152-5001.